

**HIPAA's Medical Privacy  
Rule:  
Overview and Implications for  
Research**

Phyllis C. Borzi

Research Professor

Center for Health Services Research and Policy

The George Washington University School of Public Health

# What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996
- Enacted August 21, 1996, P.L. 104-191
- Three major parts:
  - Insurance reforms
  - Fraud and abuse
  - Administrative simplification

# What Does Administrative Simplification Include?

- Transaction standards (i.e., uniformity of electronic data interchange (EDI) for common transactions, such as eligibility, claims, referrals, enrollment and disenrollment, payment)
- Medical data code set standards for use in connection with standard transactions

# Administrative Simplification, cont.

- Unique national identifiers for employers, plans, providers and individuals
- Medical privacy
- Security

# HIPAA's Dilemma

- Greater uniformity in the way standard health care transactions are handled has the potential for:
  - reducing costs for providers and health plans
  - improving the quality of care provided to patients
  - reducing medical errors

# BUT

- Once patients' medical information is stored and accessible electronically on computer networks in a universally compatible format, it is:
  - more widely accessible
  - more easily misused

# HIPAA's Statutory Mandate

- Covered entities who maintain or transmit health information must maintain reasonable and appropriate administrative, technical and physical safeguards:
  - To ensure the integrity and confidentiality of the information
  - To protect against any reasonably anticipated
    - Threats or hazards to the security or integrity of the information
    - Unauthorized uses or disclosures of the information
  - To otherwise assure compliance by the officers and employees of the covered entity

(42 USC §1320d-2(d)(2))

# Key Compliance Dates

- EDI and Medical Code Sets:
  - October 16, 2002 for covered entities
    - One year extension available if covered entity files a Compliance Plan by October 16, 2002
  - October 16, 2002 for small health plans (less than \$5 million in annual receipts)
- Medical Privacy
  - April 14, 2003 for covered entities
  - April 14, 2004 for small health plans

# What Happens If You Don't Comply?

- Penalties include:
  - \$100 per violation, \$25,000 maximum per year per standard violated
  - Criminal and civil penalties for violation of privacy standards
  - Marketplace consequences
- Enforcement rules are expected

# Privacy: What Do the Final Regulations Cover?

- Disclosure and use of protected health information
- Individual rights regarding protected health information
- Special rules for group health plan sponsors, employers and service providers to covered entities
- Special rules for hybrid entities

# What are the Basic Rules on Medical Privacy?

- “Covered entities”
- may not use or disclose
- “protected health information” (PHI)
- except:
  - with the consent or authorization of the individual who is the subject of the information, or
  - as explicitly required or permitted by the regulation

# Basic Rules, cont.

- Even if the use or disclosure is permissible, in most cases, the covered entity may only disclose the “minimum necessary” PHI to accomplish the intended purposes
- Privacy protections apply regardless of the the form of the information (electronic, oral, written)
- PHI is protected for the life of the individual and as long as the covered entity maintains the PHI

# What is a “Covered Entity”?

- Health plan
- Health care clearinghouse
- Health care provider that transmits PHI in electronic form in connection with a standard HIPAA transaction

# What is a Hybrid Entity?

- A hybrid entity is a single legal entity with:
  - at least one health care component that performs covered functions (and is therefore a covered entity)
  - one or more other components that do not engage in covered functions

# Hybrid Entities, cont.

- Under the final privacy rule, hybrid entities are those whose covered functions are not its “primary” functions
- NPRM proposes to allow any covered entity that performs both covered and non-covered functions to be a hybrid entity, even if its covered functions are primary
  - Entities could choose to be hybrid entity or treat the entire entity as a covered entity

# Hybrid Entities, cont.

- Hybrid entities must define and designate those parts of the entity that engage in covered functions and business associate functions (i.e., those that support covered functions)
  - Components that support the covered functions may be considered part of the health care component and do not need to meet the separate business associate rules

# Hybrid Entities, cont.

- Hybrid entities must create adequate separation (i.e., firewalls) between the health care component(s) and the other components of the entity
- Any use or disclosure of PHI between the health care component and the other components of the hybrid entity would be treated as a disclosure to a non-covered entity

# What is “Protected Health Information” or PHI?

- Individually identifiable information that is:
  - oral or recorded, maintained, or transmitted in any form or medium
  - created or received by a covered entity
  - Related to an individual’s past, present or future
    - physical or mental health condition
    - provision of health care
    - payment for the provision of health care

# What is “Minimum Necessary” PHI?

- Applies to uses or disclosures for payment and health care operations, not treatment
- Covered entity must adopt procedures to determine minimum necessary PHI for routine uses and disclosures
- For non-routine uses, minimum necessary PHI must be determined on a case-by-case basis

# What is “Permitted by the Regulation”?

- Generally, covered entities can use or disclose PHI without authorization for:
  - Treatment
  - Payment
  - Health care operations
- Disclosure is also permitted in certain other instances (e.g., for law enforcement purposes, for certain public health uses, when subpoenaed)
- Use or disclosure for any other purpose requires individual authorization

# What is “Treatment”?

- Provision, coordination, or management of health care and related services by one or more health care providers
- “Treatment” includes:
  - Coordination or management with a third party
  - Consultation between providers
  - Referrals from one provider to another

# What is “Payment”?

- Activities of a health plan to obtain premiums or fulfill coverage or benefit responsibilities
- Activities of a provider to obtain reimbursement

# “Payment” Activities

- “Payment” activities include:
  - Eligibility determinations and coverage decisions
  - Risk adjustment
  - Billing, claims management, collection and related data processing
  - Review for medical necessity
  - Claims adjudication
  - Utilization review
  - Disclosure to consumer reporting services

# What are “Health Care Operations”?

- Activities of a covered entity relating to covered functions, including:
  - Quality assessment and improvement
  - Licensing and credentialing
  - Underwriting and premium rating
  - Medical review, legal and compliance reviews and audits
  - Business planning, development, management
  - Customer service and internal grievances
  - Due diligence

# What's the Difference between “Consent” and “Authorization”?

- “Consent” is a broad general permission to use or disclose PHI for routine purposes (i.e., treatment, payment or health care operations)
- Covered entities may obtain consent before use or disclosure of PHI
- Any other use or disclosure of PHI requires individual authorization

# “Consent” v. “Authorization”

- Individual authorizations for use or disclosure must:
  - be specific
  - contain an expiration date
  - clearly describe individual’s right to revoke authorization
  - be signed and dated by individual
  - indicate that if disclosure to non-covered entity, PHI will no longer be protected

# What are the New Administrative Requirements for Covered Entities?

- These include:
  - designating a privacy official
  - conducting privacy training for employees handling PHI
  - establishing and enforcing reasonable privacy policies and procedures
  - establishing a complaint mechanism for disputing use or disclosure of PHI

# What New Rights Do Individuals Have?

- Review and copy PHI
- Amend and correct PHI
- Receive notice and description of covered entity's privacy use and disclosure practices
- Receive an accounting for disclosures by covered entity in prior 6 years
  - Only disclosures that were not for treatment, payment or health care operations
  - Only disclosures that were not pursuant to an individual authorization
- Initiate complaint to covered entity's privacy officer or Secretary of HHS

# **Rights of Parents as Personal Representatives of Minors**

- NPRM: Parents are presumed to be personal representatives of minor children with full access to and control of PHI of those children
- Exceptions:
  - If minor can obtain a particular health service without parental consent under state or other applicable law, the minor (not the parent) can exercise the privacy rights of individual under the final privacy rule

# Parents as Personal Representatives of Minors, cont.

- Exceptions:
  - If parent has agreed to the minor obtaining confidential treatment, the minor can control access to PHI
  - If covered provider is concerned about abuse or harm to child, the provider can refuse to recognize parent as personal representative

# Are State Privacy Laws Preempted?

- HIPAA itself, not the regulation, addresses this question
- Usual ERISA preemption principles govern
- But if state law would not be preempted by ERISA, then state laws that are “more stringent” than the privacy regulations apply
  - NPRM: State laws authorizing or requiring disclosure of PHI of minors to parents not preempted

# What about Others Who Currently Use PHI?

- Employers
- Other insurance carriers (workers' compensation, life insurance, disability)
- Service providers/vendors (such as third party administrators of group health plans, UR entities, independent medical experts, lawyers, consultants, PBMs, dental and vision plans, behavioral health vendors, etc.)
- Researchers

# Non-Covered Entities, cont.

- The final regulation contains special rules for:
  - group health plans so that employers and other plan sponsors who perform plan administration functions can have access to PHI to perform those functions
  - Business associates so that they can continue to perform services for covered entities in connection with covered functions

# Non-Covered Entities, cont.

- Section 164.512 of the final regulation also permits disclosure of PHI without the individual's written consent or authorization under certain enumerated circumstances, including:
  - To the extent the disclosure is required by law
  - If the covered entity believes the individual is a victim of abuse, neglect or domestic violence

# Non-Covered Entities, cont.

- Disclosure without written authorization permitted:
  - For certain public health activities (e.g., when the person is exposed to a communicable disease)
  - Adverse event reporting
  - For judicial and administrative proceedings
  - For research

# Use of PHI in Research

- A substantial portion of health-related research conducted today is already subject to Federal regulation through:
  - Federal Policy for the Protection of Human Subjects (“the Common Rule”), or
  - FDA’s human subject protection requirements
- HIPAA is designed to supplement these protections

# Common Rule

- Applies to all human research that is supported, conducted or regulated by 17 Federal agencies
- Includes research that uses individually identifiable health information
- Does not affect applicability of state laws protecting human subjects

# What is Human Subject Research?

- Research about a living individual about whom an investigator (including a student) conducting research obtains:
  - Data through intervention or interaction with the individual
  - Identifiable private information from any source

# Research Exempt from the Common Rule

- Research conducted in established educational settings, focused on instructional strategies, techniques, curricula, or classroom management
- Research involving use of educational tests, survey or interview procedures, or observation of public behavior UNLESS
  - Information obtained can be identified directly or through identifiers linked to subjects
  - Disclosure of responses could place the subject at risk of criminal or civil liability or be damaging to financial standing, employability or reputation

# Exempt Research, cont.

- Research involving use of educational tests, survey or interview procedures or observation of public behavior that is not exempt because of the reasons described above, if:
  - Subjects are elected or appointed public officials or candidates for public office, or
  - Federal statutes require without exception maintenance of confidentiality of PHI throughout and after research

# Exempt Research, cont.

- Research involving the collection or study of existing data, documents, records, pathological or diagnostic specimens, if:
  - Sources of data are publicly available; and
  - Subjects cannot be identified, directly or through identifiers linked to subject

# Exempt Research, cont.

- Research and demonstration projects conducted by or approved by Department or Agency heads to study, evaluate, or otherwise examine:
  - Public benefit or service programs
  - Procedures for obtaining benefits under these programs
  - Changes or alternatives to these programs
  - Changes in methods or levels of payment for benefits or services under these programs

# Exempt Research, cont.

- Research involving taste and food quality evaluation and consumer acceptance studies, if:
  - Foods studied do not contain additives, or
  - Foods studied contain ingredients at or below level and use deemed safe by the FDA, EPA or Food Safety and Inspection Service of US Dept. of Agriculture

# FDA Regulation

- Generally applies to clinical investigations under FDA jurisdiction
- Applies regardless of whether or not research is Federally funded

# Features of Common Rule/FDA Regulation

- Institutional Review Board (IRB) must review and approve proposed research projects to assure that the risks to research participants (including privacy risks) are minimized
- IRB generally requires researcher to obtain “informed consent” of human subject before research can begin
- Both regulations provide a mechanism for IRB to waive or alter informed consent requirement

# Expedited Consideration by IRB

- The Common Rule establishes expedited procedures for considering certain categories of research by the IRB (45 CFR §46.110) if:
  - Some or all of the research fits into one of these categories and is found by the IRB reviewer to involve no more than minimal risk, and
  - The request involves only minor changes to previously approved research during the 1-year approval period

# Conditions for IRB Approval

- Risks to subject are minimized
- Risks to subjects are reasonable in relation to anticipated benefits to subjects and the importance of knowledge resulting from study
- Selection of subjects is equitable
- Informed consent will be sought from each subject or authorized representative
- Informed consent will be appropriately documented
- When appropriate, research plan adequately provides for monitoring data collected to ensure safety of subjects
- When appropriate, adequate provisions exist to protect the privacy of subjects and confidentiality of data

# Waivers of Informed Consent

- Common Rule:
  - IRB can grant a waiver or alter the informed consent requirements if:
    - The research is to be conducted by or subject to the approval of state or local government officials and is designed to focus on public benefit or services programs
    - The research could not practicably be carried out without the waiver or alternation

# Informed Consent Waivers, cont.

- In addition, the IRB can grant a waiver or alter the informed consent requirements if:
  - The research involves no more than minimal risk to the subjects
  - The waiver or alteration will not adversely affect the rights and welfare of the subjects
  - The research could not practicably be carried out without the waiver or alteration
  - Wherever appropriate, the subjects will be provided with additional pertinent information after participation

# Informed Consent Waivers, cont.

- FDA:
  - Establishes different criteria for waiver of informed consent, since their rule applies to clinical research
  - Exceptions to informed consent for emergency research and for the emergency use of investigational products

# Privacy and Informed Consent

- Both Common Rule and FDA regulation require:
  - informed consent document to include a statement describing the extent to which confidentiality of records identifying subjects will be maintained
  - IRB to find that there are adequate provisions to protect privacy of subjects and confidentiality of data before research can be approved

# HIPAA, PHI and Research

- Sections 164.508 and 164.512(i) of the final regulation govern the use of PHI for research
- The rules were significantly simplified in the Notice of Proposed Rulemaking (NPRM) that was issued on March 27, 2002 (67 Fed. Reg. 14776)

# Impact of HIPAA on Research

- For research already subject to Common Rule or FDA, impact minimal
  - Some changes in way PHI can be used or disclosed
- For research involving PHI not currently subject to Common Rule or FDA, impact more substantial

# HIPAA's General Rule for Research

- PHI can be used or disclosed for research with individual authorization that meets the requirements of §164.508 of the final rule
- Individual authorization may be waived or altered for research if:
  - Research does not involve more than a “minimal risk” to privacy
  - Covered entity first obtains waiver of authorization by an IRB or Privacy Board which finds “minimal risk” under §164.512(i) of the final rule

# What is “Research” Under HIPAA?

- Definition same as Common Rule:
  - “a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge...” 45 CFR §46.102(d)
- Involves human subjects
- HIPAA applies to both living and dead subjects; broader than Common Rule

# Typical Sources of PHI for Research

- Individuals
- Medical records
- Data bases
- Other studies
- Individually identifiable health information created, maintained or transmitted by a covered entity

# De-Identified Information

- De-identified information is not PHI
- Information can be de-identified either by:
  - Removing each of 18 enumerated identifiers (safe harbor), or
  - Having an experienced statistician affirm the risk is very small that the source of the information could be identified
- Covered entity can assign a code to allow de-identification if the code is not derived from or related to information about the subject of the information

# De-Identified Information, cont.

- Final rule does not contemplate use of de-identification safe harbor for research purposes
- HHS soliciting comments on a modified approach that may be useful to researchers

# Research Authorizations

- Final rule had some research-specific requirements for authorization, particularly when research involved treatment
- NPRM proposes a single set of requirements applicable to all types of authorizations, including those for research purposes (revised §164.508(c))

# **Valid Authorizations: Core Elements**

- Description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion
- Name or other specific identification of the person or class of persons authorized to make the requested use or disclosure
- Name or other specific identification of the person or class of persons to whom the covered entity may make the requested use or disclosure

# Authorizations:

## Core elements, cont.

- Description of each purpose of the requested use or disclosure
- Expiration date or expiration event
  - If for research, “the end of the study” is sufficient
  - If for the creation and maintenance of a research database or data repository, “none” is sufficient  
(NOTE: additional authorization is needed if research involves use of information in database)

# Authorizations: Core Elements, cont.

- Signature of the individual and date
  - If signed by personal representative, must have a description of the basis for representative's authority to act for the individual
- Plain language requirement
- Required statements

# Authorizations: Required Statements

- Authorization must contain statements describing:
  - Individual's right to revoke authorization in writing and either:
    - Description of exceptions to right to revoke and how to revoke
    - Reference to provision in privacy notice that describes these features
  - The inability of the covered entity to condition treatment, payment enrollment or eligibility for benefits on the authorization, when the prohibition under the final regulation applies

# **Authorizations: Required Statements, cont.**

- The consequences to the individual of a refusal to sign the authorization when the covered entity is permitted to condition treatment, payment, enrollment or eligibility for benefits on the authorization under the final regulation (e.g., treatment can be denied, if the research is related to the treatment)
- The potential loss of privacy protection for PHI used or disclosed pursuant to the authorization through redisclosure by the recipient

# Disclosure Pursuant to Authorization: Research Involving Treatment

- Special requirements for treatment-related research in final privacy rule generally eliminated
- NPRM clarifies that:
  - Authorization form can be combined with traditional informed consent document
  - Research-related treatment can be conditioned on authorization for use or disclosure of PHI

# **Disclosure Pursuant to Authorization: Transition Rules for Research Using Existing PHI**

- Final privacy rule had different transition rules for treatment-related research and non-treatment-related research
- NPRM eliminates this distinction

# Transition Provisions for Research

- Covered entity may use or disclose PHI:
  - Created or received before and after HIPAA's compliance date
  - For a specific research study
  - If, before the compliance date, the covered entity obtained:
    - informed consent,
    - IRB-approved waiver of informed consent, or
    - express legal permission
- Covered entity can use or disclose PHI in accordance with that consent or permission until conclusion of the study

# Disclosure Pursuant to HIPAA Waiver

- Under HIPAA, a covered entity may use or disclose PHI for research purposes without an individual authorization if the covered entity first obtains either:
  - Documentation that an IRB or Privacy Board has approved the waiver of an authorization
  - Certain representations from the researcher if a request to use or disclose PHI is:
    - in preparation for research or
    - in connection with research to be conducted using only decedents' information

# IRB v. Privacy Board

- HIPAA permits a waiver or alteration of the requirement for individual authorization to be granted by an IRB or Privacy Board
- Privacy Board must:
  - Have members with varying backgrounds and appropriate professional competency
  - Include at least one member not affiliated with covered entity, entity conducting or sponsoring research, or related to any person who is affiliated with such entities
  - Not have any members participating in the review who has a conflict of interest

# HIPAA Waiver Criteria

- Waiver criteria apply to all research (whether subject to Common Rule/FDA or not)
- NPRM consolidates and simplifies criteria established in final privacy rule
- HHS intends to finalize changes by October, 2002

# HIPAA Waiver Criteria, cont.

- Use of disclosure of PHI involves no more than minimal risk to privacy of individuals, based on evidence of:
  - Adequate plan to protect identifiers from improper use and disclosure
  - Adequate plan to destroy identifiers at earliest possible opportunity consistent with conduct of research, unless there is a health or research justification for retaining identifiers or retention is required by law
  - Adequate written assurances that PHI will not be reused or disclosed to any other entity, except as required by law, for authorized oversight of the project or for other permitted research

# **HIPAA Waiver Criteria, cont.**

- The research could not practicably be conducted without the waiver or alteration
- The research could not practicably be conducted without access to and use of PHI

# Research: Special Business Associate Issues

- Can a covered entity use the business associate rules to share PHI with private sponsors of research?
  - No; not performing services for or on behalf of covered entity
- Can a covered entity use the business associate rules to share PHI with a contract research organization?
  - Yes, if performing data analysis on behalf of covered entity

# Where To Obtain Additional Information on Privacy Rule

- All press releases and fact sheets, the final regulation, and all subsequent technical guidance (including the recent Notice of Proposed Rulemaking) can be found through the web site of the agency that has responsibility for enforcing the regulations: the Office of Civil Rights at the U.S. Department of Health and Human Services
- [www.hhs.gov/ocr/hipaa/whatsnew.html](http://www.hhs.gov/ocr/hipaa/whatsnew.html)
- [www.hhs.gov/ocr/hipaa/finalreg.html](http://www.hhs.gov/ocr/hipaa/finalreg.html)