



The HIPAA Privacy Rule and Research: An Overview

Joy Pritts, JD
Research Associate Professor
Health Policy Institute
Georgetown University
jlp@georgetown.edu



Topics

- i HIPAA Background
- i Overview of Privacy Rule
- i HIPAA and Research
- i Consumer Views on Privacy Rule and Research



HIPAA: The “Act”

- i Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- i Administrative Simplification Provisions
 - 1 Encourage standardized electronic claims filing and record-keeping to reduce health care costs
 - 1 Require Congress or HHS to issue rules with respect to the privacy of individually identifiable health information



HIPAA: The Act

- i Establishes scope of who must comply with privacy standards
- i Creates preemption framework
 - ┆ Public health exception
- i Sets out penalties



Implications

Only Congress can change core scope of

- ; Who is covered by HIPAA
- ; Preemption of state law
- ; Penalties

Most privacy standards are in Privacy Rule and can be changed by HHS



Overview of Privacy Rule:

Timeline

Who Is Covered?

What Information Is Protected?

What Standards Does the Privacy Rule Set?



HIPAA: The Privacy Rule

- i First issued by HHS in December 2000
- i Modified August 2002
 - ┆ “Limited Data Sets” introduced
- i Compliance Deadline
 - ┆ April 14, 2003 (most covered entities)
- i 45 C.F.R. Parts 160 & 164



Who Is Directly Regulated?

“Covered entities”

- Health plans
- Health care clearinghouses
- Health care providers who transmit health claims-related information electronically



What Is Covered?

“Protected Health Information”

Information about a person’s:

- ; Health, health care, or payment of health care
- ; Which identifies (or could identify) the person; and
- ; Was created or received by a covered health plan or health care provider



Protected Health Information

- ⌋ Includes health information on decedents
 - ┆ Note: Common Rule only applies to living subjects

- ⌋ Excludes
 - ┆ De-identified information
 - ┆ Cells and biological tissue
 - ⌋ But *includes* analyses, communications or other identifying information related to such physical items



What Standards Does the Privacy Rule Set?

- i Establishes individuals' rights with respect to their own identifiable health information
- i Creates standards for how covered entities may "use" (internal review and communications) and "disclose" (share with others) protected health information



Individuals' Rights

- i Notice of privacy practices
- i See and copy own health information
- i Amend own health information
- i Receive an accounting of certain disclosures
- i Others



Responsibilities of Covered Entities

- i Respect individuals' rights in relation to their protected health information
- i Safeguard protected health information
- i Comply with restrictions on use and disclosure of protected health information
- i Implement "administrative" requirements



Use and Disclosure Rules

May only use” (internally) or
“disclose” (externally) PHI

- With the individual’s written authorization
- Pursuant to a provision of the Privacy Rule that expressly permits use or disclosure



Uses & Disclosures Permitted *without* Individual's Permission

- i Treatment, payment, health care operations
- i "Public interest" purposes, subject to detailed conditions
 - Public health
 - Law enforcement
 - Health oversight
 - **Research**
 - Others



Accounting of Disclosures

- i Covered entity must record and provide, upon request, an accounting of certain disclosures made within the last 6 years (after April 2003)
- i Excludes
 - ┆ Uses (internal reviews or communications)
 - ┆ Certain disclosures (e.g., treatment, payment, health care operations)
- i Generally *includes* disclosures for research



Interaction With State Laws

"Conflict Preemption"

- i Overrides provisions of state law (statutes, regulations) relating to the privacy of health information that are "contrary" to (less protective)
- i State laws that protect privacy \geq Privacy Rule remain in effect



Exception for State Public Health Laws

HIPAA does ***not*** preempt state laws that provide for the reporting of disease or injury, child abuse, birth, or death, public health surveillance, or public health investigation or intervention



Interaction with Other Federal Laws

- i Leaves in place laws that do not conflict with Privacy Rule
- i Covered entities must comply with multiple sets of laws



Enforcement

- i No personal right to sue
- i Civil penalties
 - 1 \$100 per violation/ \$25,000 maximum per year per standard violated
- i Criminal penalties
 - 1 For “knowing” wrongful disclosures
 - 1 Graduated penalties: maximum for wrongful disclosures with intent to sell/use for commercial purposes, personal gain or malicious harm
 - 1 \$250,000/ 10 year imprisonment



Enforcement

- Office for Civil Rights, HHS
- Complaint-driven
- Compliance audits
 - ┆ Authorized
 - ┆ Not currently being utilized



Enforcement: Reality Check

- i No civil fines have been assessed to date
- i Only criminal prosecutions have been for egregious “medical” identity theft



HIPAA and Research



HIPAA Privacy Rule

- i Places limits and conditions on when and how a covered entity can use or disclose health information for research



“Research” Defined

- i “A systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge.”



HIPAA and Other Research Regulations

Privacy Rule does not replace the

- 1 Common Rule (“Federal Policy for the Protection of Human Subjects”)
or
- 1 FDA Regulations on Protection of Human Subjects



How Does the Privacy Rule Generally Affect Researchers?

- i Directly—if they otherwise meet the definition of a covered entity
 - ┆ Health care provider who bills electronically
 - ┆ Health plan employee

- i Indirectly—must meet certain criteria to be able to obtain health information from a covered entity for research



Key Privacy Rule Use and Disclosure Provisions Affecting Research

- i De-identified health information is not protected by Privacy Rule
- i PHI may be used/disclosed with the individual's written permission ("Authorization")



Key Privacy Rule Use and Disclosure Provisions Affecting Research

PHI may be used/disclosed *without* authorization

- ; As a limited data set
- ; Under a waiver of the Authorization requirement
- ; Preparatory to research
- ; For research on decedent's information



De-Identified Information

All 18 identifiers removed

- ; Name
- ; Geographic subdivision smaller than a state
- ; Related dates (except year)
- ; Telephone number
- ; FAX number
- ; e-Mail address
- ; Social security number
- ; Medical record number
- ; Health plan beneficiary number
- ; Account number
- ; Certificate/license number
- ; Vehicle ID and serial numbers
- ; Device identifiers and serial numbers
- ; URLs
- ; Internet Protocol addresses
- ; **Biometric identifiers**
- ; Full face photos
- ; Any other unique identifying number, characteristic or code (except random codes, not derived from info. related to person that permit re-identification)



De-Identified Information

Statistical determination by qualified person that there is a “very small” risk that the information could be used, alone or with other reasonably available info, by recipient to identify the subject



De-Identified Information

Not protected health information
under HIPAA

- ; Restrictions on use and disclosure don't apply
- ; No requirement to account for disclosures



Research *with* Individual's Permission

Common Rule

- IRB review of research
- Informed consent for research

+ Privacy Rule

- "Authorization" to use or disclose PHI for research



Privacy Rule Authorization: Scope

- i Can pertain only to a specific research study

- i Cannot be used to give permission for
 - 1 Nonspecific research or
 - 1 Future, unspecified projects



Authorizations for Research Databases

- i Authorization can permit use/disclosure for creation and maintenance of a research database or repository
 - 1 Subsequent use/disclosure from database for a research study must be pursuant to new authorization or permitted without authorization under Privacy Rule



Authorization to Use/Disclose PHI for Research

- i Requires specific core elements and statements
 - 1 E.g., id of persons authorized to disclose and receive data, right to revoke
- i Must include expiration date/event. For research can be
 - 1 "end of research study" or
 - 1 "none"
- i Can be combined with informed consent



Authorizations & Accounting of Disclosures

- i Disclosures made pursuant to authorizations are not subject to accounting of disclosures requirements



Right to Revoke Authorization

- i Revocation is effective, except to extent that covered entity has relied upon authorization prior to revocation
- i This means that continued use/disclosure of PHI is permitted to the extent necessary to protect the integrity of the research
 - 1 Report adverse events
 - 1 Report withdrawal of patient from study



Waiver of Authorization

Covered entity may use/disclose PHI for research without authorization when it receives documentation that an Institutional Review Board (IRB) or Privacy Board has approved a waiver of the authorization required by the Privacy Rule.



Authorization Waiver Criteria

- i Similar to, yet different than, the criteria for waiving informed consent



Authorization Waiver Criteria

- i Use/disclosure involves no more than minimal risk to privacy of individual demonstrated by adequate
 - 1 Plan to protect PHI from improper use/disclosure
 - 1 Plan to destroy identifiers at the earliest opportunity consistent with conduct of research
 - 1 Written assurances that PHI will not be reused or disclosed to others except as required by law, for authorized oversight, other research permitted under Rule



Authorization Waiver Criteria

- ; Research could not practicably be conducted without the waiver
- ; Research could not practicably be conducted without access to and use of PHI



Multiple Site Research and Authorizations

- i Privacy Rule allows a waiver obtained from a single IRB or Privacy Board to be used to obtain PHI in connection with a multisite project *but also*
- i Permits covered entities to require duplicate reviews prior to disclosing PHI to researchers



Limited Data Set

Protected health information that excludes most specified identifiers, but *can* include

- ; City, state, zip code
- ; Dates
- ; Coded information and other numbers or characteristics not listed as direct identifiers



Limited Data Set

- i Can be used/disclosed for research *without* individual authorization
- i Requires a data use agreement under which recipient agrees
 - 1 Use/disclose only as agreement permits
 - 1 Use appropriate safeguards
 - 1 Not identify the info. or contact the individuals
- i Not subject to accounting of disclosures requirement



Reviews Preparatory to Research

- i Covered entities may use or disclose PHI to a researcher for activities involved in preparing for research *without* the individual's authorization



Reviews Preparatory to Research

- i Covered entity must obtain from researcher oral or written representations that
 - 1 Use/disclosure is requested solely to review PHI to prepare research protocol or similar activity prior to research
 - 1 PHI will not be removed from the premises
 - 1 PHI is necessary for the research



Identifying Research Participants

Covered entity may allow researcher (within or outside covered entity) to *identify* potential study participants as an activity preparatory to research.



Contacting Research Participants

- i Privacy Rule permits a researcher who is a workforce member of a covered entity to *contact* potential study participants (considered health care operations) for purposes of seeking Authorization.
- i Covered health care providers may discuss treatment alternatives, including participating in a clinical trial with patients.



Preparatory to Research

- i Privacy Rule's permission to contact prospective research subjects does not override Common Rule which may require such activity (if not exempt) to be reviewed and approved by an IRB and may require informed consent.



Research on Decedent's Information

- i No authorization of next of kin or waiver required under Privacy Rule
- i Must obtain representations that
 - 1 Use/disclosure is sought *solely for research on PHI of decedents*
 - 1 PHI is necessary for research
 - 1 Documentation, at request of covered entity of the death of the individuals



Patient/Consumer Views on Privacy Rule and Research

Veterans Administration Study

- Rodney A. Hayward, M.D.
 - 1 Co-PI; Director, VA Center for Practice Management & Outcomes Research
- Laura Damschroder, M.S., M.P.H.
 - 1 Co-PI, Univ. Mich., VA Center for Practice
- Michael A. Neblo, Ph.D.
 - Ohio State Univ.
- John Creswell, Ph.D.
 - Univ. of Nebraska, Lincoln



Study Aims

- i Determine the range of *informed* opinions and recommendation of veterans for optimal criteria for allowing researchers access to protected health information
 - 1 ...and how the HIPAA Privacy Rule should be interpreted and implemented



Deliberative Democracy Model

- i People are concerned about privacy
- i But they know little about:
 - 1 How or why their medical records are used
 - 1 Medical records research
- i 3 HIPAA waiver criteria are complicated and impossible to understand out of context
- i Complex and value-laden policy questions



Deliberation Protocol

- i Non-facilitated deliberation
 - ┆ Spontaneous idea generation
- i Written protocol
- i A volunteer participant helped keep their group on track
- i Privacy and research experts
 - ┆ Balanced presentations
 - ┆ Q&A



Pre-Deliberation Survey Results

- ; 39% of vets had NOT heard of the HIPAA Privacy Rule
- ; 75% of vets did not know that their medical records could be used in research without their permission
- ; 73% are very/somewhat concerned about invasion of privacy
 - ; Minorities more concerned than non-minorities



Privacy Rule Waiver Criteria

- i Most of the deliberation groups thought the following 2 factors were most important to determine “practicable”
 - 1 If the study would be less scientifically accurate
 - 1 If results would be less meaningful
- i Many participants had a strong reaction to “practicable”
 - 1 “weasel word”
 - 1 It could “mean anything you want it to



Willingness to share

Would you be inclined to allow someone to use your medical records for the following?

	Baseline	Follow-up
VA researchers conducting a study about a serious medical condition (n=160)	89%	96%
Researchers at a university conducting a study about a serious medical condition (n=146)	75%	80%



Views on Need for Authorization for Research

- Pre-deliberation

74% agree that it was critically/very important to obtain permission for each and every study

- Post-deliberation

25% wanted researchers to obtain permission for each and every study



Views on Need for Authorization for Research

Post-deliberation

- ; 40% wanted more general opt-in or opt-out model
- ; 34% thought waiver model should be kept



Findings So Far

- i Willingness to share \neq equal willingness to cede control
- i Veterans want a say in deciding how their medical records can be used for research
 - 1 ...and in *whether* their records are used
- i Veterans placed highest level of trust in VA researchers and were most willing to share their medical records with them
- i Higher trust means less stringent consent procedures



Trust Impacted by Direct Interaction with Providers

i Most do not have direct interaction with researchers

1 “A clerk couldn’t pull up your file. The doctor could. Okay. But there is a safeguard against that...”

1 “...all of these people are printing a piece of paper on you and they all have access to too much information about you.”

i ...providers, clerks, etc. are proxies for researchers



Informed Patients: Opportunity to Increase Participation

- i Wanted to know how their information had been used
 - 1 Sense of altruism
- i Consistent with findings that providing feedback to participants about research findings
 - i More likely to participate in research if they are promised feedback¹
 - 1 General
 - 1 Individual

1. Purdy, S., Finkelstein, J. A., Fletcher, R., Christiansen, C., & Inui, T. S. (2000). Patient participation in research in the managed care environment: Key perceptions of members in an HMO. *Journal of General Internal Medicine*, 15(7), 492-495.



Questions?