

HIPAA Privacy and Research



Edward B. Goldman, J.D.
University of Michigan
March 26, 2002

Theory of HIPAA Privacy



⌘ "An individual's rights and welfare must never be sacrificed for scientific or medical progress".
Comments page 974.

HIPAA Privacy Regulations



⌘ Issued: Dec. 28, 2000

⌘ Final: 04-15-01

⌘ Effective: 04-14-03

⌘ Location: 65 FR 82462-82829 OR
www.hhs.gov/ocr/hipaa/ because the
Office of Civil Rights is responsible for
implementation and enforcement.

Focus: Research



- ⌘ Research with healthy normal volunteers not subject to HIPAA (but is covered by the Common Rule 45 CFR 46 (HHS); 21 CFR 50,56 (FDA).)
- ⌘ HIPAA sets rules for research using payment or treatment data since that is protected health information (PHI).

Change from Proposed Regulations



- ⌘ The Nov. 1999 proposed regulations covered all research including “research unrelated to treatment” but the final regulations only cover research that includes treatment.
- ⌘ All research involving treatment, “regardless of the source of funding” is covered. 164.512(i)

General Issues



- ⌘ Research unrelated to treatment (not covered unless meets PHI definition)
- ⌘ Research associated with treatment (covered)
- ⌘ Medical records review (covered)
- ⌘ Medical registry review (covered)
- ⌘ De-identified records review (exempt)

Who are Covered Entities (CE)?



- ⌘ Health care providers who transmit information in electronic format including researchers who provide treatment to research participants.
- ⌘ Health plans.
- ⌘ Health care clearinghouses.

Quality Assurance Vs. Research



- ⌘ 164.501 Definitions says “Health Care Operations” includes QA, outcome studies, so long as “obtaining generalizable knowledge is not the primary purpose of any studies”.
- ⌘ Important because Health Care Operations can occur so long as they are listed in Notice and General Consent.

Research Defined



- ⌘ 164.502: "A systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge."
- ⌘ Same as Common Rule 46.102(d).

Consent and Authorization



- ⌘ "Consent" is required before creating or using PHI for treatment, payment, or health care operations. 164.506
- ⌘ "Authorization" is required to use or disclose PHI for all purposes not otherwise permitted by the rule. 164.508
- ⌘ Consent for use/disclosure may be combined with research authorization under 164.508 (f).

Compound Authorizations



- ⌘ Generally not allowed but can combine authorization for treatment with research
- ⌘ 164.508(f) requires the authorization to contain: description of information to be used; who can use; expiration date; right to revoke; right to see information; disclosure if use will result in remuneration (grants?) ; signature.

Prohibition on Conditioning



- ⌘ May not condition provision of treatment on signing authorization except may condition provision of research-related treatment on provision of authorization in accord with 164.508(f).
- ⌘ NOTE: Comments say Secretary has authority to adopt standards relating to research but no specific authorization in HIPAA itself.

Use/Disclosure for Research



- ⌘ 164.512(i) has the permitted uses rules.
- ⌘ PHI may be used for research with:
 - ⌘ 1. subject consent; OR
 - ⌘ 2. IRB approval of an alteration or waiver.
- ⌘ NOTE: Waiver not for mere convenience.
- ⌘ Waiver approval by IRB (or Privacy Board) must be documented and signed by Chair or designee.

Use for Research 2



- ⌘ Waiver criteria: 164.512(i)(2)(ii)
- ⌘ 1. No more than minimal risk to subject
- ⌘ 2. Will not adversely affect privacy/welfare of subject
- ⌘ 3. Could not practicably be conducted without waiver (feasibility test)
- ⌘ 4. Could not practicably be done without access to and use of PHI

Use for Research 3



- ⌘ Waiver criteria continued:
- ⌘ 5. Privacy risks reasonable vs. anticipated benefits and importance of knowledge reasonably expected to result
- ⌘ 6. Adequate plan to protect identifiers
- ⌘ 7. Adequate plan to destroy identifiers
- ⌘ 8. Written assurances that PHI will not be reused/disclosed except for oversight of project.

Common Rule Waiver Criteria



- ⌘ 1. No more than minimal risk.
- ⌘ 2. Will not adversely affect rights of subject.
- ⌘ 3. Could not practicably do the research.
- ⌘ 4. Subject gets added information after participation (deception research).
- ⌘ NOTE: Can waive documentation (but not consent process) under specific circumstances.

Use for Research 4



- ⌘ IRB in granting waiver must follow Common Rule plus added waiver criteria using either full or expedited review.
- ⌘ Reviews preparatory to research are allowed if researcher represents to CE that use of PHI is necessary to prepare a protocol; no PHI will be removed from the facility. 164.512 (i) (1) (ii).

Use for Research 5



⌘ Research on Decedent's information is allowed if researcher furnishes CE representation that PHI is sought solely for research and is necessary for research. CE can require date of death. Note: Common rule (45 CFR 46.102 (f)) says human subject is living individual.

Use for Research 6



- ⌘ A CE must be furnished (Query: By PI or IRB?) a brief description of the PHI for which use/access has been determined by the IRB/Privacy Board to be necessary.
164.512 (i) (2) (iii).
- ⌘ CE must also receive a statement from the IRB/Privacy Board of approval date of waiver and process (full/expedited) used.
164.512 (i) (2) (i).

Use for Research 7



- ⌘ Medical records contain PHI so they follow these rules. 45 CFR 46.102 (f).
- ⌘ If study needs to look at “thousands of records” waiver may be allowable since it would be “impracticable” to do otherwise.
- ⌘ For prospective data collection consent will be required (emergency exception).
- ⌘ Rule: Imperative to assess privacy risks for research.

De-Identification of PHI



- ⌘ 164.514 has two options on how to de-identify.
- ⌘ Once de-identified the data is not PHI.
- ⌘ Consider de-identification for research; creation of registry data.
- ⌘ Problem: Genetic or other longitudinal studies.
- ⌘ Can use random generated number to de/re-identify. 164.514 (c)

De-Identification Options



- ⌘ CE can determine that health information is not individually identifiable only if:
 - ⌘ 1. Statistician using and documenting accepted principals determines the risk of identification is “very small” OR
 - ⌘ 2. Specifically listed identifiers of individual/relatives/employers/household members are removed as follows:

De-Identification Elements



- ⌘ Names
- ⌘ All geographic subdivisions smaller than a State
- ⌘ Zip Code (can retain initial 3 digits if 20,000 plus people)
- ⌘ All dates except year
- ⌘ Phone numbers
- ⌘ Fax number

De-Identification 2



- ⌘ Electronic mail address
- ⌘ Social security number
- ⌘ Medical record number
- ⌘ Health plan beneficiary number
- ⌘ Account number
- ⌘ License/certificate number
- ⌘ Vehicle numbers

De-Identification 3



- ⌘ Device identifiers
- ⌘ Web Universal Resource Locators (URLs)
- ⌘ Internet Protocol (IP) address number
- ⌘ Biometric identifiers (finger/voice prints)
- ⌘ Full face photographic images
- ⌘ Any other unique identifier
- ⌘ Note: Can assign a code to re-identify if code is kept secure.

Who Does the De-Identification?



- ⌘ CE must de-identify. CE may assign a code to re-identify IF:
- ⌘ 1. Code is not derived from information about the individual;
- ⌘ 2. CE does not use/disclose the code for any other purpose and does not disclose the mechanism for re-identification.

164.514 (c)

Case Studies and Registries



- ⌘ Case Study uses PHI therefore needs IRB approval and patient/subject authorization (or IRB approved waiver).
- ⌘ Registries must be mentioned in Notice of Privacy and (probably) need IRB review.
- ⌘ Issues: State/Federal law mandated registries (cancer, CDC, HIV). Query: De-identification possible? Longitudinal studies.

Case Example



- ⌘ Dr. Discovery wants to conduct a family 10 year genetic study. She will collect medical records data and remove all identifiers at end of study. She says this makes the work exempt since data will be de-identified. The CE says that it must do the de-identification.
- ⌘ Who is correct? 164.514 CE must "ensure"

Case Example 2



- ⌘ Dr. Compulsive keeps in her own computer a file of every prostate surgery she has ever done including follow up. She has now developed a new surgical technique and wants to compare it to her prior cases to show it has less side effects.
- ⌘ Need IRB approval (for data and study)?

Notice of Privacy Practices



- ⌘ Facility must provide Notice.

164.520

- ⌘ Notice must describe each purpose for which PHI will be used/disclosed including research.

- ⌘ Notice must provide examples (include research, registries)

Disclosure to Subject



- ⌘ 164.528 allows an individual to have an accounting of disclosures. (Need audit trail) 164.524 allows a right of access.
- ⌘ But; 164.524(a)(2)(iii) says right of access is temporarily suspended as long as research is in progress provided the subject has agreed to the denial when consenting to participate and access is restored upon completion of the research.

Pre-Existing Consent




- ⌘ 164.532(b)(3)(ii) allows for reliance on consent for research signed prior to April 14, 2003.
- ⌘ For research that does not include treatment a pre-existing consent is valid only for PHI created before 04-14-03.

Other Stuff



- ⌘ Certificates of Confidentiality are still effective. Comments page 825.
- ⌘ Need to look at Preemption section 160.203 and your State laws.
- ⌘ Rules may change. “This...is the first step in enhancing patients’ privacy...”
Comments page 973.
- ⌘ GAO Record Linkage and Privacy Study 04-01. GAO-01-126SP.

GAO Study (April 2001)



- ⌘ "Record Linkage and Privacy: Issues in Creating New Federal Research and Statistical Information."
- ⌘ Focus: Privacy issues when multiple data bases are combined.
- ⌘ Ex: Link surveys of health status to Medicare insurance records to death records for use of insc. in last year of life.

Conclusions



- ⌘ Include research, data registries in Notice and general consent.
- ⌘ Educate IRB and faculty about medical records and registry research requirements. Consider de-identification.
- ⌘ Create protocol for IRB review and revise IRB template consent to include required elements.

Decision Tree



- ⌘ 1. Is PHI involved in a request to see/use/disclose data?
- ⌘ 2. Is there a legitimate patient care reason?
- ⌘ 3. If not is the data de-identified?
- ⌘ 4. If not are research/registries mentioned in the Notice and is there an IRB approved protocol and consent?

Decision Tree Continued



- ⌘ 5. If no consent did the IRB grant a waiver using appropriate criteria and provide required notice to CE?
- ⌘ 6. If not is some other section of HIPAA privacy applicable (reporting child abuse, data collected as mandated by non-preempted State law)? Or is HIPAA preempted by another law?

Case Example 3



- ⌘ Ima Researcher wants to study how enlarged prostate was treated 1960-80. Her protocol says she will review all medical records of admissions to the hospital for enlarged prostate cases. She requests a waiver of consent.
- ⌘ Assume the regulations are in effect. Can the IRB approve a waiver?

Case Example 4



- ⌘ The Michigan Cancer Center has always maintained a State wide registry of all cancer cases. There is a State law providing for the registry and granting it confidentiality. Post-HIPAA Privacy can the registry continue to exist? Can researchers use its data? Must they get IRB approval? Can the IRB grant a waiver of consent?
- ⌘ Preemption issues.

Case Example 5



- ⌘ Near Lee There, a third year medical student presents at teaching rounds on current hospital patients with aspergillus.
- ⌘ Issue: Need consent? IRB approval?
- ⌘ The lecture goes so well that There now wants to publish a case report.
- ⌘ Issue: Need consent? IRB approval?

Case Example 6



- ⌘ Dr. Science wants to review treatment of HIV in 1980 versus today. She proposes a chart review of 100 records from the 80's and a comparison to the next 100 cases seen. She will follow all living subjects for 5 years.
- ⌘ What should the IRB require?
(Retrospective and prospective)

Proposed Global Solution



- ⌘ Most regulatory requirements can be eliminated or safely ignored simply by terminating all patient care treatment and concentrating strictly on basic science (without animal subjects) research.

Question and Answer



- ⌘ Useful answers:
- ⌘ It depends!
- ⌘ Why do you want to know?
- ⌘ Can I get back to you on that?
- ⌘ Useful question:
- ⌘ Why didn't I listen to my parents and marry money?