

# HIPAA as it Pertains to IRBs and Research

Jeffrey M. Cohen, Ph.D., CIP  
Chief Executive Officer  
HRP Consulting Group, Inc.

# HIPAA

- Acronym for the Health Insurance Portability and Accountability Act of 1996
- Overseen by the Department of Health and Human Services (DHHS) Office of Civil Rights
- Recent modifications:
  - HIPAA Privacy Rule of 2002
  - DoD Directive 6025.18 December 19, 2002
  - Health Information Technology for Economic and Clinical Health (HITECH) Act as part of the American Recovery and Reinvestment Act of 2009 (ARRA)
  - Genetic Information Nondiscrimination Act of 2008 (GINA)
  - Final Omnibus Rule of 2013

# HIPAA

- Regulates what a **covered entity** does with Protected Health Information (**PHI**) and how it shares PHI with outside people
  - Including when a covered entity may use and disclose its PHI for research

# Use and Disclosure

- The **use** of PHI means utilization of the information by individuals **within** the covered entity
- A **disclosure** of PHI means transferring the information to a person or entity **outside** the covered entity

# Use and Disclosure

- HIPAA permits a covered entity to use or disclose protected health information, with certain limits and protections, for **treatment, payment, and health care operations** activities.
- Research is **NOT** a permitted use under HIPAA.

# PHI for Research

- Pathways to access PHI for research:
  - Signed participant authorization
  - Waiver of authorization
  - De-identified data
  - Limited data set with a data use agreement
  - Review preparatory to research
  - Research on protected health information on decedents

# Use of PHI with an Authorization Form

# HIPAA Authorization

- A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations.
- Authorizations must be written in plain language, and contain specific information regarding the information to be disclosed or used, the person(s) using or disclosing and receiving the information, expiration, right to revoke in writing, and other data.

# HIPAA Authorization and Informed Consent

- Informed consent is a process that addresses the risks and benefits of being in a study
- HIPAA authorization addresses the risk to the subject's privacy and how the subjects' data will be used and disclosed

# Authorization for Future Research

- Requirement to describe **each purpose** for which PHI will be used or disclosed does not mean that the authorization must be limited to a specific study/studies
- Authorization can be obtained **upfront** for **non-specific future research** provided that adequate description is given for an individual to reasonably expect the future use

# Conditioned Authorization

- Covered entity may condition provision of **research-related treatment** (e.g., clinical trial intervention) on an individual's provision of authorization to use or disclose PHI for **that** research activity
- All other research authorizations must be unconditioned – cannot require an individual, in order to participate in a clinical trial, to authorize use/disclosure of PHI for a **different** research activity (e.g., data/tissue repository)

# Compound Authorization

- HIPAA authorizations for various research activities may be combined in a **single document** with one another and with informed consent or any other written permission for research, provided that:
  - Any conditioned authorization (e.g., for a clinical trial intervention) and unconditioned authorization (e.g., for a data/tissue repository) are clearly differentiated; **and**
  - The individual has the opportunity to opt in to the research activities described in the unconditioned authorization (e.g., data/tissue repository)

# Invalid Authorization

- Note that HIPAA authorization is not valid if:
  - Expiration date has passed
  - Any one of the core elements is missing, including subject signature or date
- Unlike with informed consent, there is no waiver of documentation for HIPAA
  - Must meet the HIPAA waiver criteria to bypass a defective authorization

# Uses of PHI Without an Authorization

# Waiver of the Authorization Requirements

- Similar to process and criteria for waiving informed consent under 45 CFR 46
  - Requires written documentation of approval by privacy board or IRB
  - Waiver determination by IRB or privacy board may be done on expedited basis
- DoD Directive 6025.18 limits waivers of authorization to research involving minimal risk

# Waiver of the Authorization Requirements

1. The use or disclosure of the PHI involves no more than **minimal risk to privacy** based on the presence of the following elements:
  - An adequate plan to destroy identifiers at the earliest opportunity;
  - An adequate plan to protect health information identifiers from improper use and disclosure;
  - Adequate written assurances that the PHI will not be reused or disclosed to (shared with) any other person or entity

# Waiver of the Authorization Requirements

2. The research **could not** practicably be conducted without the waiver or alteration
3. The research **could not** practicably be conducted without access to and use of PHI

# De-identified Information

# De-Identified Information

- De-identified health information is not PHI, and therefore *is not* protected by the Privacy Rule

# De-Identified Information

- Data is de-identified if:

- **Expert Determination**

- A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods determines or renders the information not individually identifiable

- **Safe Harbor**

- The 18 HIPAA identifiers have been stripped

# HIPAA Identifiers

1. Names
2. Geographic subdivisions smaller than state
  - Exceptions for first three digits of zip code
3. All elements of dates (except year) for dates directly related to an individual, such as:
  - Birth date
  - Admission and discharge dates
  - Date of death
  - All ages over 89 and all elements of dates indicative of such age
  - Ages 90 and over can be aggregated into single category
4. Telephone numbers
5. Facsimile numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web universal resource locators (URLs)
15. Internet protocol (IP) address numbers
16. Biometric identifiers, including fingerprints and voiceprints
17. Full-face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification

# Limited Data Sets

# Limited Data Sets and Data Use Agreements

- Limited data sets can be used and disclosed without written authorization or waiver of authorization, but only with data use agreements
- Because limited data sets may contain identifiable information, they are considered PHI

# Limited Data Sets

- The following identifiers must be stripped:
  - Names
  - Postal address information other than city, state and zip code
  - Telephone numbers
  - Fax numbers
  - E-mail addresses
  - Social security numbers
  - Medical record numbers
  - Health plan beneficiary numbers
  - Account numbers
  - Certificate/ license numbers
  - Certificate/ license numbers
  - Vehicle identifiers and serial numbers, including license plate numbers
  - Device identifiers and serial numbers
  - URLs
  - IP addresses
  - Biometric identifiers, including finger and voice prints
  - Full-face photos

# Data Use Agreement

- Used to obtain satisfactory assurances that the recipient of the limited data set will use or disclose the PHI in the data set only for specified purposes

# Data Use Agreement

- Must include:
  - Specific permitted uses and disclosures of the limited data set by the recipient
  - Identify who is permitted to use or receive the limited data set

# Data Use Agreement

- It must also include stipulations that the recipient will:
  - Not use or disclose the information other than as permitted by the agreement
  - Use appropriate safeguards to prevent other use or disclosure and report any such use or disclosure to the covered entity
  - Hold any agent of the recipient to the standards, restrictions and conditions stated in the agreement
  - Not identify the information or contact the individuals

# “Minimum Necessary” Restriction

- Uses or disclosures of PHI must be limited to the information reasonably necessary to accomplish the purpose of the sought or requested use or disclosure
  - True for HIPAA waivers, limited data sets; not applicable with specific authorization
- If certain information is not needed for a study, do not collect it

# Preparatory to Research

- No authorization is needed if the covered entity obtains from the researcher representations that:
  - The use or disclosure is requested solely to review PHI as necessary to prepare a research protocol;
  - The PHI will not be removed from the covered entity; *and*
  - The PHI requested is necessary for the research

# Research on Decedents' PHI

- No requirement to obtain authorization from the legally authorized representative or next of kin
- But, the covered entity needs to obtain from the researcher who is seeking access to decedents' PHI:
  - Oral or written representations that the use and disclosure is sought solely for research on the PHI of decedents;
  - Oral or written representations that the PHI for which use or disclosure is sought is necessary for the research purposes; **and**
  - Documentation (at the covered entity's request) of the death of the individuals whose PHI is sought

# References

- 45 CFR 160: General Administrative Requirements. Department of Health and Human Services.  
[http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title45/45cfr160\\_main\\_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title45/45cfr160_main_02.tpl)
- 45 CFR 164: Security and Privacy. Department of Health and Human Services.  
[http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title45/45cfr164\\_main\\_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl)
- DoD Directive 6025.18, "Privacy of Individually Identifiable Health Information in DoD Health Care Programs," December 19, 2002

# References

- Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the HIPAA Privacy Rule. Office for Civil Rights. 2012.  
[http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs\\_deid\\_guidance.pdf](http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf)
- HHS Announces Proposed Changes to HIPAA Privacy Rule. Press Release. Department of Health and Human Services 2012.  
<http://www.hhs.gov/news/press/2011pres/05/20110531c.html>
- 78 FR 5566: Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act and GINA. *Federal Register*. 2013.  
<http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf>
- Barnes, Mark, et al. *HIPAA and Human Subjects Research: A Question-and-Answer Reference Guide*. Waltham, MA: Barnett International, 2003.

# References

- New Rule Protects Patient Privacy, Secures Health Information. Press Release. Department of Health and Human Services. 2013.  
<http://www.hhs.gov/news/press/2013pres/01/20130117b.html>
- HIPAA—Frequently Asked Questions. Office for Civil Rights. 2013.  
<http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html>
- HIPAA Privacy: Research. Office for Civil Rights. 2013.  
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/>