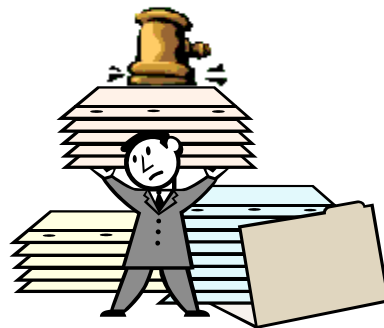


2013 Changes to HIPAA Regulations

Kris West, J.D., M.S.

Office of Research Compliance



Presentation Outline

- HIPAA
 - Changes in the HIPAA Regulations Affecting Research
- New HIPAA Breach Notification Standard

Changes to the HIPAA Rules

- New regulations published January 25, 2013
- Effective Date: March 26, 2013
- Compliance Date: September 23, 2013
- Rule Location:
<http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf>

Changes Affecting Research

- Compound Authorizations
- Authorization of Future Research Use or Disclosure
- Decedents Information
- Sale of Protected Health Information

Compound Authorization

- **Old Rule:**
- A research authorization can't be combined with another research authorization if the Covered Entity conditions provision of the treatment or payment for treatment on the individual's signing the other authorization.
- Example: The HIPAA authorization for a person who enrolls in a CT in which the research-related treatment is conditioned on the individual's signing the research authorization for the clinical trial, can't be combined with another research authorization such as authorization to store biological materials in a research repository. The person would need to sign one authorization for the clinical trial and one for the banking of materials.

Compound Authorization

- **New Rule**
- Conditioned and unconditioned activities can now be described in one authorization.
- Authorization must clearly distinguish between conditioned and unconditioned activities.
- Authorization must permit participant to opt-in to unconditioned research activity; opt-out provision is not permitted.

Compound Authorizations

- New rule does not apply to research involving psychotherapy notes.
- Authorizations for the use or disclosure of psychotherapy notes can't be combined with any other authorization.

Compound Authorization

Example

- Under new rule, authorization can include authorization for use of PHI in a clinical trial (i.e., participant must authorize use of PHI in order to participate in the trial) and authorization for optional biospecimen banking.

Authorization for Future Research

- **Old Rule:**
- HIPAA did not permit authorization for purposed of future research.
- Caused conflict with Common Rule which permitted informed consent to future research.

Authorization for Future Research

- **New Rule:**
- Authorization for purpose of future research is now permitted.
- HOWEVER, authorization still must describe the future research adequately so that the participant will know what to expect as to how the PHI will be used/disclosed.
- Description of PHI may include that collected beyond time of original study.

Decedents' Information

- **Old Rule:**
- Decedent's information was covered by HIPAA without time limit.
- Could use decedent's information for research on decedents by signing data use agreement stating that person was dead and describing research use.

Decedent's Information

- **New Rule:**
- PHI of a decedent is no longer considered to be PHI after the decedent has been dead for 50 years.
- Rule regarding use of decedent's information per data use agreement still applies to persons who have not yet been deceased for 50 years.

Sale of PHI

- **New Rule:**
- With limited exceptions, covered entities cannot sell PHI without authorization.
- Research Exception:
 - PHI may be sold for research purposes if remuneration received is a reasonable cost-based fee to cover costs to prepare and transmit the information.
 - Cost can cover labor, materials, supplies.
 - Profit margin not allowed.

Sale of PHI

- De-identified data not subject to “no sale” rule.
- Limited Data Sets are subject to “no sale” rule.

Breach Notification: HITECH

- HITECH – Health Information Technology for Economic and Clinical Health Act
- New regulations include change in breach notification standard.

Breach Notification

- **Old Rule:**
- Notification to individuals of Breach of Privacy required if:
 - the unauthorized disclosure, use, acquisition or access compromises the security or privacy of the protected health information by posing a significant risk of financial, reputational or other harm to the individual.

Breach Notification

- **New Rule**

- Harm standard removed
- Focus is on whether or not the PHI was compromised.
- No more exceptions for limited data sets that don't contain dates of birth or zip codes.
- Encryption is still a safe harbor.

Breach Notification

- **New Standard**
- Assess probability that PHI has been compromised based on a risk assessment that considers:
 - The nature and extent of the PHI involved, including types of identifiers and likelihood of re-identification
 - Unauthorized person who used the PHI or to whom it was disclosed.
 - Whether the PHI was actually acquired or viewed.
 - Extent to which risk to the PHI has been mitigated.

Breach Notification

- Contents of Notice:
 - What happened?
 - Date of breach and discovery of breach.
 - Type of health info involved.
 - Steps individual should take to protect themselves.
 - What is being done to investigate and mitigate harm.
 - Identify contact person who can provide info & answer questions.

Questions?

- Kris West. Office of Research Compliance
- kwest02@emory.edu
- (404) 727-2398