United States Department of Health & Human Services
Office of the Secretary
Office for Civil Rights (OCR)

HIPAA/HITECH Omnibus Final Rule

Secretary's Advisory Committee on Human Research Protections

March 2013

Christina Heide, JD
Senior Health Information Privacy Policy Specialist
HHS Office for Civil Rights

Omnibus Rules

- Final Rule on HITECH Privacy, Security, & Enforcement Provisions (and certain non-HITECH changes) (proposed rule published July 2010)
- Final Rule on new HITECH CMP Structure (interim final rule published Oct. 2009)
- Final Rule on HITECH Breach Notification (interim final rule published Aug. 2009)
- Final Rule on GINA Privacy Provisions (proposed rule published Oct. 2009)

Omnibus Components

- **HITECH Privacy & Security**
  - Business associates
  - Marketing & Fundraising
  - Sale of PHI
  - Right to request restrictions
  - Electronic access
- **HITECH Breach Notification**
- **HITECH Enforcement**
- **GINA Privacy**
- **Other (non-statutory) Modifications**
  - Research authorizations
  - Notice of privacy practices (NPP)
  - Decedents
  - Student immunizations

Today's Focus

- Compound authorizations for research
- Authorizations for future research
- Period of protection for decedents
- Sale of protected health information (PHI)
- Breach notification
- Business associates (BA)

Important Dates

- Published in Federal Register – January 25, 2013
- Effective Date – March 26, 2013
- Compliance Date – September 23, 2013
- Transition Period to Conform BA Contracts – Up to September 22, 2014, for Qualifying Contracts

Research Authorizations – Old Rule

- Compound Authorizations
  - Not permitted for use/disclosure of PHI for conditioned and unconditioned research activities (e.g., separate authorization forms required for use/disclosure of PHI in a clinical trial and storage of PHI in a biorepository)
- Future Use Authorizations
  - Not permitted; authorizations for research must include descriptions that are study specific

Research Authorizations – New Rule

- Compound Authorizations
  - Single authorization form permitted for use/disclosure of PHI for conditioned and unconditioned research activities, with clear opt in for voluntary (unconditioned) component
  - Flexibility permitted on ways to differentiate the components
- Future Use Authorizations
  - Permitted so long as authorization for future research purposes includes adequate description such that it would be reasonable for the individual to expect his or her PHI could be used or disclosed for the research
- Better aligns with Common Rule informed consent requirements

Decedent Information

- Old Rule
  - Health information about decedents generally protected in same manner/extent than that of living individuals
- New Rule
  - Decedent's information is no longer PHI after 50-year period

Sale of PHI – Old Rule

- Covered entities prohibited from “selling” patient information; however, no general prohibition on receiving remuneration for disclosure of PHI that is otherwise permissible

Sale of PHI – New Rule

- Even where disclosure is permitted, CE is prohibited from disclosing PHI (without individual authorization) in exchange for remuneration
- If authorization obtained, authorization must state that disclosure will result in remuneration
- Limited research exception -- remuneration must be limited to cost to prepare and transmit PHI

Definition of Breach – Old Rule

- Impermissible use or disclosure of (unsecured) PHI which compromises the security or privacy of the information
  - Compromises means poses a significant risk of financial, reputational, or other harm to the individual
- To determine if must notify, preamble stated CE/BA must perform risk assessment, based on at least:
  - What type or amount of PHI was used or disclosed
  - Who received/accessed the information
  - Potential that PHI was actually accessed or acquired
  - What steps were taken to mitigate
- Exceptions for inadvertent, harmless mistakes
- Narrow exception for limited data sets without dates of birth & zip codes

Definition of Breach – New Rule

- Harm standard removed
- New standard – impermissible use/disclosure of (unsecured) PHI *presumed* to require notification, unless CE/BA can demonstrate low probability that PHI has been compromised based on a risk assessment of at least:
  - Nature & extent of PHI involved
  - Who received/accessed the information
  - Potential that PHI was actually acquired or viewed
  - Extent to which risk to the data has been mitigated
- Exceptions for inadvertent, harmless mistakes remain
- Exception for limited data sets without dates of birth & zip codes removed

Business Associates – Old Rule

- Covered entities may disclose PHI to BAs provided there is a contract in place to protect the information
- No direct liability on BAs for misuse of information or lack of safeguards
- Researchers not BAs by virtue of research activities (although they may become BAs in some other capacity)

Business Associates – New Rule

- BAs must comply with the technical, administrative, and physical safeguard requirements under the Security Rule; directly liable for violations
- BAs must comply with the use or disclosure limitations expressed in BA contract and those in the Privacy Rule; directly liable for violations
- Subcontractors of BA are now defined as BAs
  - BA liability flows to all subcontractors
- Researchers still not considered BAs by virtue of research activities
  - Preamble also clarifies that IRBs are not BAs by virtue of their research review, approval, and oversight functions

For More Information

www.hhs.gov/ocr/privacy/