# The HIPAA Omnibus Final Rule:
## Overview and Implications for AF4Q Alliances

Jane Hyatt Thorpe, JD
Lara Cartwright-Smith, JD, MPH

March 13, 2013

THE GEORGE WASHINGTON UNIVERSITY
SCHOOL OF PUBLIC HEALTH AND HEALTH SERVICES
The Department of Health Policy

# Agenda

- Introductions
- About the Project and Website
- HIPAA Omnibus Final Rule Overview and Implications
- Discussion

# Legal Barriers Project

- Scope: research and analysis re: actual and perceived legal barriers to health system transformation
- Funded by RJWF since 2006
- Key Staff:
  - Sara Rosenbaum, JD
  - Jane Hyatt Thorpe, JD
  - Lara Cartwright-Smith, JD, MPH
  - Taylor Burke, JD, LLM
  - Devi Mehta, JD, MPH
  - Elizabeth Gray, JD
  - Grace Im, JD

# www.HealthInfoLaw.org

- Health system transformation (especially quality improvement and delivery system reform) depends on use and exchange of health information
- Valuable resource covering:
  - All federal and state laws relating to the use and exchange of health information
  - Analyses of emerging issues in state and federal law affecting the transformation of the health care system
  - Content: brief summaries of state and federal laws, comparative analyses, and longer, in-depth analyses, presented in multiple formats for a variety of audiences

# HIPAA Refresher

- Privacy Rule
  - A covered entity cannot use or disclose protected health information unless it is permitted or required by the Rule
  - And then (generally) only the minimum necessary information may be used or disclosed
  - Rule sets a federal floor (more protective state statutes are permitted)
- Security Rule
  - Prescribes administrative, technical, and physical safeguards covered entities must use re: electronic protected health information.

# HIPAA Refresher

- Breach Notification
  - Requires notification from covered entities and their business associates following a breach of unsecured protected health information.
- Enforcement
  - Penalties for violations up to $1.5m based on level of culpability

# HITECH Act

- Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of the American Recovery & Reinvestment Act of 2009 (ARRA)
- Made changes to HIPAA, especially with respect to business associate liability, accounting for disclosures, breach notification, sale of PHI, use of PHI for marketing and research, and enforcement
- Required significant rulemaking by HHS between 2009 and 2013, culminating in Omnibus Final Rule released Jan. 17, 2013 (published in Federal Register Jan. 25, 2013): http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

# Genetic Information Nondiscrimination Act of 2008 (GINA)

- Statute prohibits the use of genetic information by health plans for underwriting purposes
- Requires changes to HIPAA Privacy Rule to specifically protect genetic information as protected health information, included in Omnibus Final Rule

# Omnibus HIPAA Final Rule

- Includes 4 rulemakings:
  1. Final rule implementing modifications to the HIPAA Privacy, Security, and Enforcement Rules as required by HITECH that was included in a proposed rule on July 14, 2010.
  2. Final rule implementing changes to the HIPAA Enforcement Rule as required by HITECH that was published as an interim final rule on October 30, 2009.
  3. Final rule implementing changes to the Breach Notification for Unsecured Protected Health Information as required by HITECH that was published as an interim final rule on August 24, 2009.
  4. Final rule modifying the HIPAA Privacy Rule as required by GINA that was published as a proposed rule on October 7, 2009.
- Deadline for compliance is September 23, 2013 in most cases
  - (Updates to existing business associate and data use agreements may take an additional year)

# Privacy Rule Changes

- Direct liability for business associates (BAs)
  - Prior to HITECH, HIPAA Rules governed covered entities (CEs); business associates were not penalized for HIPAA noncompliance, only for breach of contract with CE
  - Now, BAs directly liable for certain Privacy Rule requirements.
- Expanded definition of business associate ("creates, receives, maintains, or transmits PHI on behalf of CE or BA and otherwise meets definition of BA"):
  - Now includes:
    - HIO, e-Prescribing Gateway, or other that provides data transmission services for PHI to a CE
    - Entity offering a PHR to individuals on behalf of a CE
    - Subcontractors of BAs

# Privacy Rule Changes (cont'd)

- New Limitations on Use and Disclosure
  - Marketing
  - Fundraising
- Sale of PHI Prohibited without Individual Authorization
  - Sale of PHI = Disclosure of PHI by CE or BA where the CE or BA directly or indirectly receives remuneration from or on behalf of the recipient in exchange for the PHI.
    - Limited data set not exempted
- Expanded rights of individuals to restrict use, disclosure, access

# Privacy Rule Changes (cont'd)

- Modified Notice of Privacy Practices requirements to reflect changes in HITECH, GINA, and Final Rule
- Genetic information = PHI
- Separate authorization required for conditioned and unconditioned activities (i.e., treatment and unrelated research activity, such as tissue banking)
- Privacy rule applies to decedent's PHI for 50 years after death
- "Patient safety activities" included in definition of "health care operations"

# Security Rule Changes

- Minimal changes, but now applies to BAs
- BAs directly liable for compliance with:
  - Administrative, physical and technical safeguards;
  - Policies and procedures under Security Rule
- For example, BAs must:
  - Conduct a Security Rule risk assessment
  - Establish a Risk Management program
  - Designate a Security Official

# Breach Notification

- Breach = impermissible "acquisition, access, use, or disclosure of PHI" that "compromises the security or privacy of PHI"
- Replaced "harm" threshold of 2009 IFR with more objective standard. CEs must consider:
  1. Nature and extend of PHI involved
  2. Persons to whom disclosure made
  3. Whether PHI was actually acquired or viewed, and
  4. Extent to which the risk of breach to PHI has been mitigated
- Impermissible use or disclosure presumed to be a breach unless low probability info was compromised
- Must notify (HHS, media, BAs) within 60 days of discovery

# Enforcement and Penalties

- HHS required to:
  - Formally investigate any complaint if possibility of willful neglect;
  - Impose civil monetary penalties if violations due to willful neglect not cured within 30 days
- 30 day time to cure begins on date of actual or constructive knowledge (determined on case-by-case basis)
- CEs and BAs liable for their agents
- Tiered Liability
  - Did Not Know = $100-$50,000 per violation, $1,500,000 max cal. year
  - Reasonable Cause = $1,000-$50,000 per violation, $1,500,000 max cal. year
  - Willful Neglect, Corrected = $10,000-$50,000 per, $1,500,000 max cal. year
  - Willful Neglect, Not Corrected = $50,000 per, $1,500,000 max cal. year

# What This Means for AF4Q Alliances

- You must know your status under HIPAA and have appropriate business associate agreements in place
- If you are a BA, you must take appropriate actions to comply with the Privacy and Security Rules
- Don't forget to check and comply with relevant state law requirements if more stringent than HIPAA, as well as other federal laws (e.g., Part 2 protection of substance abuse information)
- Always consider individual authorization/consent for data collection, research activities, patient care teams

# Looking Ahead

- We will continue to expand resources available at www.healthinfolaw.org.
  - HIPAA materials available now:
    - Shorter overview
    - Section-by-section analysis
    - Tables showing side-by-side comparison of proposed and final rules
  - 50 state comparative maps to be posted shortly
  - Sign up for our mailing list if you would like to be notified of new content, tools, and publications