New HIPAA Rules and EHRs: ARRA & Breach Notification

Jim Sheldon-Dean
Director of Compliance Services
Lewis Creek Systems, LLC
www.lewiscreeksystems.com
and
Raj Goel
Chief Technology Officer
Brainlink International, Inc.
www.brainlink.com

Today's Objectives

- Learn about the changes to HIPAA and how they impact the use of EHRs
- What's in the HIPAA Breach Notification Rule?
- What are the deadlines and what's my plan?
- Agenda:
  I. How ARRA Impacts HIPAA
  II. Changes to HIPAA Practices
  III. Implementation Schedule
- Disclaimer: We are not lawyers and this is not legal advice – we are only providing information and resources

I. Health Information and the Stimulus Package (ARRA)

A. Origins of Changes to HIPAA
B. New Definitions
C. Types of Impacts on HIPAA

A. Origins of Changes to HIPAA

- New kinds of entities holding health information
- Objections to some uses of health information
- Lack of breach notification for health information
- Lack of control over business associates
- Enforcement seen as lacking teeth

New Law Developed in 2008

- Health Information Technology for Economic and Clinical Health Act, or the HITECH Act
- Under consideration already in 2008
- Became Title XIII of the American Recovery and Reinvestment Act of 2009, or ARRA, signed February 17, 2009
- Title XIII, Subtitle D-Privacy
  - Definitions: § 13400
  - Part 1–Improved Privacy Provisions and Security Provisions: § 13401-13411
  - Part 2–Relationship to Other Laws, Regulatory References, Effective Date, Reports: § 13421-13424

B. New Definitions - § 13400

- Breach
- Electronic Health Record
- Personal Health Record

New Definition § 13400(1) - Breach

- Unauthorized acquisition, access, use, or disclosure
- Compromises privacy or security of PHI
- Except if info cannot reasonably be retained
- Does not include unintentional or inadvertent acts by employees or staff
  - in good faith and within scope of job
  - without further acquisition, access, use, or disclosure

New Definition - § 13400(5) Electronic Health Record

- An electronic record of health-related information
- Created, gathered, managed, and consulted by clinicians and staff
- § 3000(13) Qualified Electronic Health Record
  - Includes patient demographic and clinical health information, such as medical history and problem lists
  - Has the capacity to:
    - Provide clinical decision support
    - Support physician order entry
    - Capture and query information relevant to health care quality
    - Exchange electronic health information from other sources

New Definition - § 13400(11) Personal Health Record

- Electronic record of "PHR Identifiable Health Information" per § 13407(f)(2)
  - Provided by or on behalf of the individual
  - Identifies the individual
- Drawn from multiple sources
- Managed by or for the individual
- e.g. Google Health, Microsoft Health Vault, etc.

C. Types of Impacts on HIPAA (1 of 2)

- New kinds of entities covered
  - Business Associates now under HIPAA
  - Personal Health Records
  - Health Information Exchanges
- New information handling requirements
  - Breach Notification
  - Accounting of Disclosures from EHR
  - Electronic copy of PHI from an EHR

C. Types of Impacts on HIPAA (2 of 2)

- New limits on disclosures of PHI
  - To insurers, by request
  - Minimum necessary
  - For sale
  - For marketing
- New audits, enforcement, and penalties
  - Wrongful disclosures
  - Willful neglect
  - Audits mandated
  - Increased Penalties

II. Changes to HIPAA Practices

A. Breach Notification

B. Accounting of Disclosures

C. Restriction of Disclosures

D. Access to PHI in EHRs

A. Breach Notification (1 of 5)

- In ARRA/HITECH: § 13402
- Interim Final Rule published August 23, 2009, effective September 23, 2009, enforceable February 22, 2010
- CFR 45 Part 164 Subpart D
- HIPAA Breach Notification Rule: § 164.4xx
- http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf
- Co-equal with Privacy and Security Rules
- Compliance must be integrated with that for State laws
  - must meet requirements of both
  - the stricter rule applies
  - may mean multiple notices
- Similar law for PHRs under § 13407, administered by Federal Trade Commission

A. Breach Notification (2 of 5)

- § 164.400 Effective for breaches of unsecured PHI on or after 9/23/2009
- § 164.402 Breach is acquisition, access, use, or disclosure that poses a significant risk of financial, reputational, or other harm to the individual
- You must make the call on “significant risk of harm”
- What is “unsecured”?
  - Guidance on HHS Web site per ARRA/HITECH § 13402(h)(2)

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html

  - Refers to NIST guidance
  - Look for FIPS 140-2 compliance
  - Old electronic media must be cleared
  - Old hard copies must be unreadable; redaction is excluded

A. Breach Notification (3 of 5)

- § 164.404(a) Notify individual if breach of unsecured information in violation of Privacy Rule
  - Considered discovered on first day known (or should have been)
- § 164.404(b) Notify without delay, max 60 days
- § 164.404(c) Content of Notice (in plain language)
  - What happened, date of breach and discovery
  - What information was breached
  - What steps the individual should take for protection
  - What the CE is doing about it
    - Investigating the incident
    - Mitigating impacts
    - Protecting against future incidents
  - Contact information
    - Toll free number, E-mail and postal address, Web site

A. Breach Notification (4 of 5)

- § 164.404(d) Method of Notice
  - To the individual by mail, or e-mail if individual prefers; multiple mailings OK
  - If known to be deceased, to next of kin
  - If no contact info for more than 10, then post on web site home page for 90 days or major media, with toll-free number active for 90 days
  - Contact also allowed by phone if urgent
- § 164.406 Notification to Media
  - If more than 500 in any jurisdiction, must notify prominent media outlets serving the area
  - Without unreasonable delay, max. 60 days
  - Same content as individual notice

A. Breach Notification (5 of 5)

- § 164.408 Notification to Secretary of HHS
  - If over 500, notify HHS when you notify the individuals
  - Secretary of HHS will post >500s on the HHS web site
  - Annual report to Secretary of HHS of *ALL* breaches
- § 164.410 BAs must notify CEs
  - Without unreasonable delay, within 60 days
  - Who affected and information needed for contact
- § 164.412 May delay for Law Enforcement
- § 164.414(a) Must comply with Privacy Rule re training, complaints, sanctions, policies, documentation, etc.
- § 164.414(b) Burden of proof is on CE to show notice was given and any determination of “not a breach”

B. Accounting of Disclosures

- § 13405(c): New rules for EHRs
  - Privacy rule has exception for TPO
  - TPO exception for accounting will no longer apply when an EHR is used
    - Accounting of EHR disclosures goes 3 years back
  - Can list disclosures by CE and BA, or list CE disclosures and identify the BAs to ask for an accounting
  - Individuals can ask BAs directly for an accounting
  - Secretary of HHS shall define standards and regulations
  - If using EHR prior to 1/1/09, effective 1/1/2014
  - If began using EHR after 1/1/09, effective 1/1/2011

C. Restriction of Disclosures

- § 13405(a) Individual may request no disclosure of services to insurer if paid for out of pocket by the individual
  - must comply
  - effective 2/17/10
- EHR will need to track any such services

D. Access to PHI in EHRs

- § 13405(e) Individual may request electronic copy of EHR information
- effective 2/17/10
- How will this be provided?
  - Readable, understandable
  - Delivery method?
  - Encryption?

III. Implementation Schedule

A. Sections in Effect Immediately
B. Sections in Effect During 2009
C. Sections in Effect 2/17/2010
D. Longer-term Deadlines
E. Your to-do list…

A. Sections in Effect Immediately

- Higher Penalties
  - $100 - $50,000 per instance, for unintentional, unpreventable violations
  - $1000 - $50,000 per instance, for reasonable cause but not willful neglect
  - $10,000 - $50,000 per instance, for willful neglect that is corrected
  - At least $50,000 per instance for willful neglect that is not corrected
  - Up to $25K to $1.5 million per year for all violations of the same type
- State Attorneys General may enforce HIPAA

B. Sections in Effect During 2009

- Breach Notification
  - Interim final rule effective September 23, 2009
  - Log all breaches beginning 9/23/2009, for report on 2009 due March 1, 2010
  - Guidance issued by HHS April 17, 2009, available on the HHS Web site
  - FTC regulation for PHR breach notification issued August 17, 2009

C. Sections in Effect 2/17/2010

- February 17, 2010
  - Business Associates covered by HIPAA
  - HIEs, RHIOs, etc. become BAs
  - ➢Restriction of disclosure to insurers
  - Disclose only minimum necessary
  - Guidance on de-identification due
  - ➢Providing copy of EHR in electronic format
  - Marketing limitations
  - Wrongful Disclosures penalties in effect
  - ➢Audits of HIPAA compliance by HHS under way

D. Longer-term Deadlines

- February 22, 2010: Breach rule enforceable
- March 1, 2010: 2009 Breach log due at HHS
- August 17, 2010
  - Regulations on sales of PHI due, eff. 6 months later
  - Regulations on Willful Neglect due, eff. 6 months later
  - Guidance on “minimum necessary” due
- January 1, 2011
  - If began using EHR *after* 1/1/09, must be able to provide accounting of disclosures *including* TPO
- January 1, 2014
  - If began using EHR *before* 1/1/09, must be able to provide accounting of disclosures *including* TPO

E. Your to-do list…

- ✓Don’t be in denial – willful neglect will cost you
- ✓Establish good information security practices as required by the HIPAA Security Rule
- ✓Start developing your breach notification policy and plans *now* – you should have this for state laws and the FTC Red Flags Rule as well – and start logging breaches *now*
- ✓Be ready by February 2010 for:
  - ✓restriction of disclosures to insurers
  - ✓electronic copy of PHI from EHR
  - ✓compliance with HIPAA Breach Notification Rule
  - ✓increased HHS audits

Thank you!

- Any Questions?
- For additional information, please contact:

Jim Sheldon-Dean, **Lewis Creek Systems, LLC**
jim@lewiscreeksystems.com www.lewiscreeksystems.com
802-425-3839
and
Raj Goel, **Brainlink International, Inc.**
raj@brainlink.com www.brainlink.com
917-685-7731

- Resources, regulations, laws, guidance, and tools at:
  www.lewiscreeksystems.com/resources.html