HIPAA and HITECH Compliance Under the New HIPAA Final Rule

Presented by:
Barry S. Herrin, CHPS, FACHE
Smith Moore Leatherwood LLP
Atlanta GA
(877) 404-7466 x1027
barry.herrin@smithmoorelaw.com

HIPAA Final Omnibus Rule ("Final Rule")

- Issued on January 17, 2013
- Published in the Federal Register on January 25, 2013
- Becomes effective on March 26, 2013
- Compliance date for most provisions – September 23, 2013

What the Final Rule Changes

- Definition and Obligations of Business Associates
- Requirements for Breach Notification
- Certain Privacy Rule Provisions
- Enforcement
- GINA

Definition of a Business Associate ("BA")

- Now includes any entity that creates, receives, transmits, or ***maintains*** PHI on behalf of a covered entity
  - 42 C.F.R. § 160.103

Definition of a Business Associate ("BA")

- Includes health information organizations, e-prescribing gateways, patient safety organizations, subcontractors, and entities offering personal health records on behalf of a covered entity

Definition of a Business Associate ("BA")

- Does not include health care provider who receives disclosures from a covered entity concerning the treatment of an individual with respect to those disclosures
- Does not include "conduits" – entities and organizations that only transmit (without altering or storing) PHI
  - Internet ISPs are not "conduits" if they save copies of emails
  - What does this do for enterprises that permit use of iPads and iPhones?

Definition of a Business Associate ("BA")

- Does not include government agencies that receive PHI for the purpose of either determining eligibility for or enrollment in a government health plan administered by another government agency or collecting PHI for such purposes
  - Social Security, Medicare, Medicaid, TRICARE are these kinds of entities
  - Recall that disclosures to the government to determine compliance were exempted originally from HIPAA restrictions

Definition of a Business Associate ("BA")

- Researchers, financial institutions, and malpractice insurers are not BAs while performing their normal activities, BUT they may become BAs if performing a function, activity, or service for a covered entity that falls within the definition of a BA

Definition of a Business Associate ("BA")

- Researchers who create de-identified or limited data sets for a Covered Entity → BAs
- Financial institutions that perform accounts receivable functions on behalf of a Covered Entity → BAs
- Malpractice insurers that access PHI to perform risk management or risk assessment activities on behalf of a Covered Entity → BAs

Definition of a Business Associate ("BA")

- Question: Are physical and cloud storage companies that do not routinely access PHI now BAs?
  - What if the storage companies do not access the PHI?
  - What if the storage companies are not aware that their servers or facilities are being used to store PHI?

Compliance Obligations of Business Associates

- The Final Rule confirms that both (1) BAs and (2) BAs' subcontractors who use PHI in performing services for those BAs may be directly liable for complying with many of the HIPAA privacy and security requirements and subject to penalties for noncompliance.
- Compliance down the contractual chain - Covered Entity with BA, BA with subcontractor, subcontractor with its subcontractor, etc.
  - But covered entities do not have to enter BAAs with their BAs' subcontractors
  - Covered entities must determine the level of supervision they want to dedicate to BA activities.

Deadlines for BAA Compliance

- BAAs now need to comply with the Final Rule.
- Covered entities need to review and evaluate their BAAs to ensure that they comply with the Final Rule.
- Existing BAAs that comply with current (pre-Final Rule) HIPAA requirements and are not modified between March 26 and September 23, 2013 may continue until the earlier of:
  1. the date the BAA is renewed or modified; OR
  2. September 22, 2014
- New BAAs must comply with the Final Rule's requirements by September 23, 2013.

Changes to Breach Notification Requirements

- HHS – old subjective risk of harm standard gave too much discretion to covered entities and BAs
- Final Rule → new, "more objective" definition of breach
- New standard takes effect on September 23, 2013
  - Before then, can use the subjective risk of harm standard from the HITECH interim final rule

Changes to Breach Notification Requirements

- "Breach" = impermissible acquisition, access, use, or disclosure of unsecured PHI
- The new standards PRESUME a breach has occurred and that notification is required, UNLESS
  - an exception applies; or
  - the covered entity or BA demonstrates that there is a low probability that the PHI was compromised

Changes to Breach Notification Requirements

- Factors for determining the probability that the PHI was compromised:
  - Nature and extent of PHI involved
  - The unauthorized person who impermissibly used the PHI or to whom the PHI was impermissibly disclosed
  - Whether the PHI was actually accessed or viewed
  - The extent to which the risk to the PHI has been mitigated

Changes to Breach Notification Requirements

- Clarification: For breaches affecting fewer than 500 individuals, covered entities and BAs must notify HHS within 60 days after the end of the calendar year in which the breaches were discovered, not when the breaches occurred
  - Reminder: A breach is "discovered" as of the first day on which the entity knew or should have known through the exercise of reasonable diligence that a breach occurred

Changes to the Privacy Rule

- Fundraising
- Marketing
- Sale of PHI
- Research
- Right to Access Copies of Electronically Stored PHI
- Right to Request Restrictions on Uses and Disclosures
- Notice of Privacy Practices
- Decedents
- Immunization Records

Fundraising

- The following categories of information may now be used or disclosed for fundraising communications:
  - Demographic information
  - When health care was provided to the individual
  - The departments in which the individual was treated
  - Treating physician's name
  - Information about outcomes (including death or suboptimal treatment)
  - Health insurance status

Fundraising

- Individuals must be offered a "clear and conspicuous" opportunity to pt out of future fundraising solicitations through a means that would not be unduly burdensome on the individual or carry more than a minimal cost
  - OCR suggestion: Opt-out by e-mail, toll free or local phone calls, or return of pre-paid postcard

Fundraising

- Covered entities can decide whether to offer individuals a blanket opt-out of receiving all future fundraising communications or campaign-specific opt-outs
  - But, cannot condition treatment or payment on a individual's decision to opt-out
  - And cannot send fundraising communications to individuals who have opted-out
- Covered entities must also provide a process for individuals to opt back in
  - Effect: Greater responsibility for tracking individuals' opt-out decisions

Marketing

- Broader definition of "marketing"
  - any treatment or health care operations communication to an individual about health-related products or services
  - for which a covered entity or its BA receives financial remuneration
  - from a third-party in exchange for making the communication

Marketing

- Must receive monetary remuneration to be a marketing communication
  - Nonfinancial remuneration → not marketing
- Remember – authorization is required for <u>all</u> marketing communications
  - Under the Final Rule, authorization is required whenever a covered entity or BA receives $ from a third party for making a marketing communication (even if it's about new or alternative treatments)

Right to Access ePHI

- If an individual requires an electronic copy of PHI that the covered entity maintains electronically in one or more designated record sets ("ePHI"), the covered entity must provide access to the ePHI in the electronic form and format sought by the individual

Right to Access ePHI

- ***Limitation***: ePHI must be readily producible in that form and format
  - If not possible to produce it in that format, the covered entity and the individual must agree on a readable electronic format in which the information will be provided
  - If the individual does not agree to accept the ePHI in the available electronic formats, the covered entity must provide a hard copy

Right to Access ePHI

- No requirement that covered entities purchase new systems or software to provide ePHI in a form or format that is not readily producible
  - ***However, covered entities whose systems cannot produce ePHI in any electronic form may need to purchase software or hardware to allow them to offer some form of an electronic copy***
- Covered entities that maintain hybrid records do not have to scan paper documents in order to provide electronic copies of those records

Right to Access ePHI

- Covered entities may provide copies of ePHI via unencrypted emails IF:
  - they notify the individual of the possible risks involved (e.g., that a third party may read and access the ePHI); AND
  - the individual decides to receive the ePHI via an unencrypted email rather than through another available electronic means

Right to Access ePHI

- If requested by a individual, a covered entity must transmit a copy of PHI directly to a third party.
  - Request must:
    - Be signed;
    - Clearly identify the third party; and
    - Clearly identify where to send the information

Right to Access ePHI

- Costs of providing PHI to individuals
  - May charge a reasonable, cost-based fee for providing copies
  - Includes labor costs for copying
    - Staff time to create and copy electronic files
  - Includes fees for supplies used in creating electronic media (discs and flash drives) if portable media requested
  - Includes postage incurred on behalf of individuals who request mailing of electronic media

Right to Access ePHI

- Fees cannot include:
  - Costs for maintaining systems or new technology
  - Retrieval fees for electronic copies (also not permitted for paper copies)
- Remember, cannot charge more than state law allows
  - No connection between the typical "per page" charge state statutes have and these new concepts
  - Assume each "page" of data is a printed page unless guidance to the contrary is received

Right to Access ePHI

- Shorter time frame for responding to access requests for ePHI
  - 60 days total
    - 30 days with a single 30 day extension if provide written notice to individual that states the reason for the delay and the expected date of completion
  - Even when ePHI is stored off site
    - This should increase interest in instituting and maintaining a document destruction policy

Right to Request Restrictions

- HITECH requires covered entities to agree to an individual's request to restrict uses and disclosures of his/her PHI related to a treatment or service IF:
  - The request is to restrict disclosure of information to the individual's health plan for payment or health care operations purposes AND
  - The individual agrees to pay the covered entity for the treatment out of pocket and in full

Right to Request Restrictions

- Final Rule clarifies that:
  - Not necessary to create separate medical records or otherwise segregate PHI that is subject to such a restriction, but do need to flag this restriction in the record to assure the information is not provided to the health plan for other operations purposes
  - If the restriction requested is for a service that is part of a bundle of services provided in a single encounter, should counsel the individual about whether it is able to unbundle the service to permit payments for just that one service and the possible effect of doing so
    - if unbundling the service is possible, the provider should abide by the request to unbundle
    - if it is not possible, the provider should permit the individual to restrict and pay out of pocket for the entire bundle of services

Right to Request Restrictions

- Final Rule clarifies that:
  - No obligation to inform downstream providers of a restriction, but covered entities are encouraged to counsel patients to request a restriction and pay out of pocket with downstream providers
  - Providers within an HMO who cannot by law accept payment from an individual in excess of the individual's cost-sharing amount ***may counsel individuals to use an out-of-network provider to obtain items or services about which the individual wishes to restrict PHI from disclosure***
- The Rule specifically sanctions behaviors that used to indicate benefit fraud – how will this affect the life insurance industry?

Notice of Privacy Practices

- Must update notice of privacy practice ("NPP") to address several changes including:
  - most uses and disclosures of psychiatric notes, marketing communications, and the sale of PHI are not permitted without prior written authorization
  - must notify affected individuals of a breach of unsecured PHI
  - if applicable, may opt out of receiving any fundraising communications from the provider or plan
  - individuals may restrict disclosures of PHI to health plans where they have paid out of pocket and in full for such care

Decedents

- Definition of PHI excludes information for individuals who have been dead more than 50 years
- Can disclose a decedent's PHI to family members or others who were involved in the decedent's care or payment for that care before the decedent's death
  - Unless the disclosure would be inconsistent with a preference expressed by the decedent to the covered entity before death
  - Disclosure of PHI – limited to what is relevant to the person's involvement in the decedent's care or payment for the care

Immunization Records

- May disclose student immunization records to schools when the schools are required by law to have this information before admitting students with oral or other agreement from the student (if of age) or the student's parent or guardian
- Must document that agreement was given
- If do so, written authorization is not required
- Agreement is effective until revoked

Enforcement

- BAs and their subcontractors – subject to civil monetary penalties and enforcement actions
- If a preliminary review of facts cited in a complaint about a HIPAA violation indicates a possible violation due to willful neglect → the HHS Secretary must investigate

Enforcement

- Audits:
  - If the facts indicate a possible violation due to willful neglect → the HHS Secretary must complete a compliance review
  - If the facts do not indicate a possible violation due to willful neglect → the HHS Secretary has discretion to decide whether to investigate further/do a compliance review
- HHS Secretary has discretion to move directly to a civil monetary penalty without exhausting informal means of resolution

Enforcement

- Penalties
  - Implements HITECH's tiered civil monetary penalty structure for violations occurring on or after February 18, 2009:
  - $100 to $50,000 per violation and up to $1.5 million for identical violations occurring during a calendar year
  - Sanctions depend on
    - whether "willful neglect" is present
    - whether the covered entity or BA "did not and, by exercising reasonable diligence, would not have known that a violation occurred"

Genetic Information (GINA)

- Genetic information = type of health information
- Prohibits most health care plans from using/disclosing genetic information for underwriting purposes
  - Excludes long-term care plans
  - Plans must include this in their Notice of Privacy Practices
- Genetic information – manifestation of a disease/disorder in an individual's family member and genetic tests of an individual and family members
  - But once a disease manifests itself in the individual, no longer considered genetic information

QUESTIONS?