The HITECH NPRM: Expansion of HIPAA’s Protections for EHR Privacy and Security, and Impact on Health Plans and Healthcare Providers

Co-sponsored by the Health Information and Technology (HIT); Hospitals and Health Systems (HHS); Physician Organizations (Physicians); and Payors, Plans, and Managed Care (PPMC) Practice Groups

August 31, 2010 · 1:00-3:00 pm Eastern

Presenters:
Adam H. Greene, JD, MPH
U.S. Department of Health and Human Services
Washington, DC · adam.greene@hhs.gov

Christina M. Heide, JD
U.S. Department of Health and Human Services
Washington, DC · christina.heide@hhs.gov

Paula M. Stannard, Esquire
Alston & Bird LLP
Washington, DC · paula.stannard@alston.com

Moderator:
Patricia A. Markus, Esquire
Smith Moore Leatherwood LLP
Raleigh, NC · trish.markus@smithmoorelaw.com
Initial Reactions and Implementation Planning

Paula M. Stannard, Esquire
Alston & Bird LLP
Washington, DC • paula.stannard@alston.com
Overview

- Initial Reactions to the Proposed Rule
  - Subparts A & B
  - Enforcement Rule Changes
  - Privacy Rule Proposals

- Implementation Planning – It’s Not Too Soon to Start
  - Business Associates (and Subcontractors)
  - Policies and Procedures
  - Workforce Training
  - Notice of Privacy Practices
  - Authorizations
  - Marketing and Fundraising
Initial Reactions: Subparts A & B

- Compliance Dates for Implementation of New or Modified Standards and Implementation Specifications, §160.105
  - Creates a uniform compliance date of 180 days after the effective date of the standards or implementation specifications unless otherwise provided.
    - Applies to both new and modified standards and implementation specifications.
  - Implications for covered entities (CEs) (and business associates (BAs)) with respect to future rules.
Initial Reactions: Subparts A & B

- Subcontractors As Business Associates, § 160.103(3)(iii)
  - The Statutory Framework for Applicability and Civil Liability under HIPAA §§ 1172 and 1176.
  - HITECH §§ 13401 and 13404’s Changes to Applicability and Civil Liability.
  - Direct Regulation and Civil Liability or Indirect Regulation and Contractual Liability?
  - Implications for Subcontractors of Business Associates.
Initial Reactions: Enforcement Rule Changes

- Resolution of Complaints by Informal Means, § 160.312(a)(1)
  - Current rule provides that if an investigation or compliance review indicates noncompliance, “the Secretary will attempt to reach a resolution of the matter satisfactory to the Secretary by informal means.”
  - Proposed rule provides that “the Secretary may attempt to reach a resolution of the matter satisfactory to the Secretary by informal means.”
  - The proposed revision will likely hold implications for covered entities and business associates.
Initial Reactions: Enforcement Rule Changes

- **Covered Entity Liability for Actions of Agents Who Are Business Associates, § 160.402(c)**
  - Proposed rule would eliminate a current exception from the liability of CEs for CMPs for violations resulting from acts of agents that excepts the CE from liability if
    - the agent is a BA
    - there is a compliant BA agreement in place, and
    - the CE did not (1) know of the pattern of activity or practice of the BA and (2) did not fail to act as required by the Privacy or Security Rule with respect to such violations.
  - Proposal increases CE’s potential exposure for violations of BAs.
  - Implications: Need for CEs to undertake due diligence with respect to BAs and vendors and to audit BAs’ activities.
Initial Reactions: Enforcement Rule Changes

Factors in Determining Amount of CMP, History of Prior Compliance, Including Violations, § 160.408(c)(1) & (2)

- Current rule provides that prior history of compliance includes “[w]hether the current violation is the same or similar to previous violation(s)” and “[w]hether and to what extent the covered entity has attempted to correct previous violations.”
- Proposed rule would substitute “indications of noncompliance” for “violations.”
- “Indication of noncompliance” seems vague and ambiguous.
  - What is it?
  - What quantum of evidence is necessary to establish an “indication of noncompliance”?
- Implications for covered entities and business associates.
Initial Reactions: Privacy Rule Proposals

- Marketing, §164.501
  - Implements certain exceptions to the marketing authorization requirement: (1) certain health care operations communications, unless the CE receives payment from a third party; (2) refill reminders; (3) treatment communications subsidized by third parties.
  - How will CEs distinguish between treatment and health care operations disclosures?
  - How will the opt-out provisions work with respect to treatment communications to a patient?
Initial Reaction: Privacy Rule Proposals

- Sale of PHI, § 164.508(a)(4)
  - What is “direct or indirect remuneration”? What does not constitute “direct or indirect remuneration”?
  - An exception is provided for the sale of the CE’s business and related due diligence. Should a similar exception be provided for sale of a BA’s business and related due diligence?
  - Many CEs outsource various functions to BAs. Exceptions and explanations should be drafted such that they cover the excepted activity regardless of whether the activity is performed by the CE or a BA.
Initial Reaction: Privacy Rule Proposal

- **Minimum Necessary, § 164.514**
  - HITECH § 13405(b)(2) provides that, with respect to disclosures of PHI, “the covered entity or business associate disclosing such information shall determine what constitutes the minimum necessary to accomplish the intended purpose of such disclosure.”
  - It is not clear if OCR intends to address this provision in the guidance that it is to issue under HITECH § 13405(b)(1)(B) – or if it believes that the provision sunsets with § 13405(b)(1)(A).
  - It is important to know how the provision interacts with the regulatory provisions at § 164.514(d)(3)(iii) which permit the CE to rely on certain requested disclosures as the minimum necessary for the stated purpose.
Initial Reactions: Privacy Rule Proposal

Fundraising, §164.514

- Implements the HITECH Act’s requirement that a CE provide the recipient of a fundraising communication a clear and conspicuous opportunity to opt-out of receiving further fundraising communications, as well as making several additional changes.
  - What constitutes a clear and conspicuous opportunity to opt-out?
  - How is a CE to ensure that no fundraising communications are sent to an individual who has opted-out? Does this proposed requirement impose an unrealistic obligation on a CE?
Initial Reactions: Privacy Rule Proposal

- Right to Request Restrictions, § 164.522(a)
  - The preamble to § 164.522(a)(1)(vi)(B), on the mandatory restriction, emphasizes that, if the individual fails to pay in full for the treatment or service, the provider is under no obligation to restrict the information.
  - The interaction of this provision with § 164.522(a)(2)(iii)(A), barring the provider from unilaterally terminating a mandatory restriction, is ambiguous and could cause confusion to CE as well as patients.
  - OCR is requesting comments on whether covered health care providers should be to notify downstream providers of any restrictions.
    - Such a requirement would be extremely burdensome on providers.
    - To what extent will CEs have to make “reasonable efforts” to secure payments?
Initial Reaction: Privacy Rule Proposal

- Right to Access, §164.524
  - Section 13405(e) of HITECH requires CEs that use or maintain an EHR to give individuals the right to obtain a copy of their DHI in an electronic format.
  - OCR cites section 264(c) of HIPAA to expand requirement to apply to CEs that maintain PHI “electronically in one or more designated record sets…”
  - Does OCR have authority to broaden this requirement?
  - Implications for CEs.
Implementation Planning: It’s Not too Soon to Start

- Planning for implementation and compliance does not have to wait for a final rule.
- You can begin to identify and prioritize implementation tasks based on the provisions of the proposed rule and current/proposed compliance and transition dates.
- Finalize your plan when the final rule is published.
- The following are a few concrete ideas on implementation planning.
Implementation Planning: Business Associates and Subcontractors

- CEs (and BAs) should:
  - Consider whether, as a result of the revised definition of "business associate," there are entities for which new BA (or BA subcontractor) contracts are needed.
  - Create or update a list of BAs and BA contract expiration dates.
  - Prioritize, consistent with proposed transition provisions, the order in which BA contracts will need to be amended.
  - Develop a check list of provisions to be added to BA contracts.
  - Consider whether, and what type of, due diligence should be undertaken with respect to BAs (or subcontractors).
Implementation Planning: Policies and Procedures

- Based on the proposed rule, are there policies and procedures that will need to be adopted?
- Review and identify existing policies and procedures that will likely need to be revised. For example:
  - Fundraising
  - Marketing
  - Minimum Necessary
  - Responding to Requests for Restrictions
  - Research
  - Access of Individual to PHI
- Prioritize development and revision of such policies and procedures.
Implementation Planning: Workforce Training

- Based on proposed rule and list of policies and procedures likely needing revision, identify the areas in which new or revised training modules will likely be needed.
- Prioritize development of such training modules based on relative importance of topic.
- Identify and prioritize the categories of workforce members who will need to receive such training.
Implementation Planning: Notice of Privacy Practices

- CEs may have as little as 60 days to revise and distribute/begin to distribute revised Notices.

- Create a checklist of likely topics to be added to the Notice, including:
  - Fundraising and right to opt out
  - Right to request restrictions on use/disclosure of PHI and when a CE cannot deny such request
  - Breach notification obligations
  - Subsidized treatment communications and opt-out right
  - Description of uses and disclosures that require authorization and, a statement that uses and disclosures not described in the notice would be made only with authorization
Implementation Planning: Authorizations

- Identify those types of authorizations that will likely need revision, such as
  - Research:
    - Compound authorizations and language on anti-conditioning rule.
    - Authorization regarding future research.
  - Marketing
  - Sale of PHI
- Develop/prioritize the development of such revised authorizations.
Implementation Planning: Marketing and Fundraising

- If applicable, develop model language for marketing and fundraising communications to inform of right to opt out.
- Consider mechanisms by which individuals will be able to opt out of fundraising solicitations easily and without undue burden: 800 number, email address, website functionality.
- Consider mechanism by which individuals can opt back in to fundraising solicitations.
- Consider methods to strengthen processes to ensure that individuals who have opted out of fundraising solicitations do not receive such communications.
Questions?