Legal and Privacy Implications of the HIPAA Final Omnibus Rule

February 19, 2013

Pillsbury Winthrop Shaw Pittman LLP

Faculty

Gerry Hinkley
Partner
Pillsbury Winthrop Shaw Pittman LLP

Deven McGraw
Director, Health Privacy Project
Center for Democracy & Technology

pillsbury

Status of Federal Privacy Regulations

- Health Information Technology for Economic and Clinical Health Act, the "HITECH Act"
  - Interim Final Rule (Data Breach) August 24, 2009
  - Interim Final Rule (Enforcement) October 30, 2009
  - Notice of Proposed Rulemaking (HITECH Rule) July 14, 2010 – including Enforcement
- Genetic Information Nondiscrimination Act of 2008 ("GINA")
  - Notice of Proposed Ruling (GINA Rule) October 7, 2009
- Omnibus Rule (Data Breach, Enforcement, HITECH, GINA) published January 25, 2013, effective March 26, 2013

Scope of the Omnibus Rule

- Revised breach notification standard
- Patient access to information contained in an electronic health record
- Regulation of business associates (“BAs”) and subcontractors
- Limitations on use/disclosure of PHI for marketing without authorization
- Prohibition on “sale” of PHI without authorization

Scope of the Omnibus Rule

- Research uses of data – compound, more general authorizations
- Patients' right to restrict data sharing with payors
- Requirements to modify and redistribute notices of privacy practices
- Inclusion of limitations on use of genetic information for underwriting
- Clarifies HHS Secretary's role in enforcement, imposition of civil money penalties (CMPs) and CMP liability for acts of agents

What's not in the Omnibus Rule

- Accounting of Disclosures – still in process
- Methodology for giving individuals "harmed" by HIPAA violations a percentage of any civil monetary penalties or settlements collected (HITECH Section 13409(c)(3)) – no rule proposed yet
- Office for Civil Rights (OCR) also late on report re: privacy protections for PHRs not covered by HIPAA and guidance on implementation of minimum necessary standard
- HITECH also mandated study of definition of "psychotherapy notes" – no specific deadline for the study

Implementation of Omnibus Rule

- Majority of the HITECH statutory provisions took effect on February 18, 2010, but no enforcement by federal regulators without rules
- Omnibus Rule is effective on March 26, 2013 (60 days from publication) (“Effective Date”)
- Enforcement rule changes are effective March 26, 2013
- Covered entities and business associates have 180 days from Effective Date (September 23, 2013) to come into compliance (“Compliance Date”), includes GINA compliance
- If no changes made prior to September 22, 2014, Business Associate Agreements must come into compliance by that date (“Limited Deemed Compliance Date”)

Breach Notification

- HITECH established right of individual to be notified of breaches of PHI
- Breach = the "unauthorized acquisition, access, use or disclosure of [PHI] which compromises the security or privacy of such information…"
- Exceptions include inadvertent, good faith access or disclosures within a CE/BA if the data is not further subject to unauthorized use

IFR Breach Notification Standard

- Interim Final Rule (IFR) – CEs/BAs must notify of breaches of unsecured PHI that cause a significant risk of harm to the data subjects
  - Harm includes financial & “other” harm; standard was controversial
  - Data correctly encrypted per NIST standards is not “unsecured PHI”
- Exceptions included limited data set with “extra” deletions

Omnibus Rule Breach Notification Standard

- Definition of “breach” is changed from IFR definition
- An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate demonstrates there is low probability that the PHI has been “compromised”
- Determining whether or not there is a low probability data has been “compromised” requires analysis of what happened (or may have happened) to the data
- Limited data set exception deleted

Breach Notification – Risk Assessment

- CE/BA should perform risk assessment post-breach discovery and must consider at least the following:
  - Nature and extent of PHI involved, including types of identifiers and likelihood of re-identification
  - Who was the recipient of the PHI
  - Was the PHI actually acquired or viewed
  - The extent to which the risk to misuse of the PHI has been mitigated

Breach Notification – Burden of Proof

- If no risk assessment performed, the default is notification
- Burden of demonstrating low probability that PHI is compromised is on the CE/BA
- Decision not to notify must be documented in case of review

Breach Notification – Obligations to Notify

- CEs must notify individuals (although can delegate this to BAs)
- BAs must notify CEs
- Subcontractors must be obligated to notify their contracting partner so the information can go back up the chain

Breach Notification – Examples of Risk Analysis Criteria

- Likelihood of identification or re-identification:
  - a list of patient names – not low probability
  - patient discharge data, patient not specified – can patients be re-identified? – could be low probability (depends on the circumstances)
- Who is the unauthorized recipient:
  - a HIPAA covered entity – low probability, as long as you have evidence the risk has been mitigated
  - an employer – may be able to use personnel records to re-identify – not low probability
- PHI actually acquired or viewed:
  - untampered with laptop – low probability
  - information mailed to wrong person – not low probability
- Has improper use been mitigated:
  - satisfactory assurances of destruction from a known person – low probability

Breach Notification – What Did Not Change

- Definition of “Unsecured Protected Health Information”
- When a breach is treated as “discovered”
- Timeline for notifications
- Content of notification
- Methods of notification
- Notification to the media and the Secretary (minor modification – counting from year of discovery)
- Notification by Business Associate
- Delay requested by law enforcement
- Documentation and burden of proof
- Pre-emption standard regarding state laws

Patient Access to Electronic Health Information

- If PHI held electronically, individual entitled to an electronic copy if in a "designated record set" (not just the information in an "EHR")
- Must be in the format requested if "readily producible;" if not, in a readable electronic form and format agreed upon by the entity and the individual
  - Not required to buy new software to do this – but must have capability to provide some electronic copy
  - If individual declines to accept electronic formats entity makes available, can default to hard copy
  - Not required to accept patient's device – but can't require individuals to purchase a device from you if they don't want to

Patient Access – Reasonable Safeguards

- Must have reasonable safeguards in place to protect transmission of ePHI – but…
  - If an individual wants information by unencrypted e-mail, entity can send if they advise the individual that such transmission is risky
  - Must have a secure mechanism – can't force individuals to accept unsecure
- Omnibus Rule allows up to 60 days (30 days less); preamble urges entities to make information available sooner when possible

Patient Access – Third Parties, Charges

- Individuals can have the copy directed to another person/entity – but the choice must be in writing and clearly identify the individual/entity
  - Information must be protected and entity must implement reasonable policies and procedures to send it to the right place (e.g., type e-mail correctly)
  - "In writing" can be electronic
- Fees charged are restricted to labor costs – cannot include costs of retrieval, or portion of capital costs
- Charge can include supplies provided to individual upon request

Business Associates/Subcontractors

- Omnibus Rule conforms HIPAA regulations to HITECH Act changes
  - Before HITECH, BAs regulated through business associate contracts or agreements ("BAAs")
  - After HITECH, BAs and subcontractors are regulated directly under HIPAA
    - Must comply with Security Rule (rule is flexible to accommodate small BAs)
    - Must comply with some of Privacy Rule and provisions of BAA

BAs – Expanded Regulation

- Expanded definition of "business associate“
  - “Business associate” means one who, on behalf of a covered entity, creates, receives, maintains or transmits PHI
  - "Business associate" now also means "subcontractor of business associate“ who creates, receives, maintains or transmits PHI on behalf of a business associate
  - Status as BA based upon role and responsibilities, not upon who are the parties to the contract
- Implications for subcontractor relationships
  - Contract between the covered entity's BA and that BA's subcontractor must satisfy the BAA requirements
  - Subcontractor of subcontractor is also a BA, and so on
  - As a result, HIPAA/HITECH obligations that apply to BAs also directly apply to subcontractors

BAs – Clarifications

- Rule clarifies definition of "business associate" -- included:
  - Patient Safety Organizations
  - Health information exchange organizations, e-prescribing gateways, covered entities' personal health record vendors (not all PHRs)
  - Data transmission providers that *require access to PHI on a routine basis*
- Not included – those who just provide transmission services, like digital couriers or "mere conduits"
  - However, those who store PHI, even if they don't intend to actually view it, are BAs (implications for cloud model EHRs)

BAs – Uses of PHI

- Uses of PHI
  - BAs may use or disclose PHI only as permitted by BAA or required by law
  - BAs may not use or disclose PHI in manner that would violate Privacy Rule
  - Subcontractors subject to limits in initial CE-BA agreement – must pass along in subcontracts
  - BAs not making a permitted use or disclosure if not following minimum necessary rules
- BA does not comply if it knows of subcontractor's material noncompliance and does not take reasonable steps to cure the breach or, if such steps fail, to terminate the relationship

BAs – Consequences

- Secretary authorized to receive and investigate complaints against BAs (including subcontractors), and to take action regarding complaints and noncompliance
- BAs (incl. subs) required to maintain records and submit compliance reports to Secretary, cooperate in complaint investigations and compliance reviews, give Secretary access to information
- BAs (incl. subs) forbidden to intimidate, discriminate against, etc. those who make complaints, cooperate with regulators or oppose unlawful actions
- BAs (incl. subcontractors) subject to civil money penalties for HIPAA violations
- BA/subs remain liable under contract to CE/BA

BAs – Transition Provisions

- Generally, compliance required 180 days following Omnibus Rule's effective date (3/26/13), which is 9/23/13
- Additional time allowed to enter into conforming business associate agreements (Limited Deemed Compliance Date)
  - If BAAs comply with pre-Omnibus rule, parties have 1 additional year to bring their BAAs into compliance with Omnibus Rule (9/22/14)
  - If BAAs do not comply with pre-Omnibus rule (or no BAA exists), must enter into BAAs that comply with Omnibus Rule by 9/23/13
  - Regardless of compliance deadlines, compliance with Omnibus Rule required when existing BAAs renew or are modified
  - BAAs not otherwise modified or renewed prior to 9/22/14 must be brought into compliance by that date

Marketing Pre-HITECH

- In public surveys of privacy concerns, marketing uses of data (esp. health and other sensitive data) rank very high
- Pre-HITECH: Marketing uses of PHI required prior patient authorization; however, communications sent by CEs for treatment or to recommend additional benefits or services were not marketing

Marketing – Omnibus Rule

- Significant change from Notice of Proposed Rulemaking (NPRM): prior authorization from patient required for using or disclosing PHI where the CE or BA receives financial remuneration for making a marketing communication from the third party whose product or service is being pitched
- Abandoned NPRM's distinction between communications for treatment and those for "operations;"
- If financial remuneration by or on behalf of the manufacturer whose product/service is being pitched to the covered entity or its business associate, the communication is marketing and requires prior patient authorization
- Authorization must disclose that the communication is paid for
- Covered entities can use a general authorization for all such communications or do it on a case-by-case basis

Marketing – Exceptions

- Refill reminders exception
  - Remuneration allowed for currently prescribed drug or biologic; includes generics
  - Remuneration must be reasonably related to cost of making the communication (cannot make a profit)
- Face-to-face communications remain exempt with no requirement for any remuneration to be reasonable (related to labor, supplies and postage)
- Communication consisting of promotional gifts of nominal value provided by the covered entity remain exempt

What counts as "Financial Remuneration"?

- Direct or indirect payments count; in-kind benefits do not count
- Payment must be for making the marketing communication; payments to implement programs (such as disease management programs) do not trigger marketing authorization requirements
  - However, assumption is that the communication urges participation in the program, not the use or purchase of the third-party's product or service
- General health promotions or communications regarding eligibility for public programs – even if subsidized- are not marketing

Fundraising

- Fundraising – use of PHI to promote the entity (not to benefit a third party)
- Expanded types of PHI able to be used for fundraising – includes department of service, treating physician, and outcome
- Requires clear and conspicuous opt-out, that must be honored
- Can notify of opt-out in initial communication; can do overall opt-out as well
- Cannot condition treatment on patient's decision

Sale of PHI

- Authorization generally required, with notice that disclosure of PHI is in exchange for payment; includes non-financial benefits
- Exceptions
  - Public health
  - Research purposes – remuneration must be reasonably related to the cost of preparing and transmitting information (can include indirect costs but cannot make a profit)
  - Treatment and payment – disclosure of PHI to receive payment is not a "sale" of PHI
  - Corporate transactions
  - Disclosures to business associates
  - Disclosures to the individual
  - Disclosures required by law
  - Other disclosures permitted by the rules, provided remuneration is related to cost of making the disclosure

Research

- Researchers have sought changes to both HIPAA and the Common Rule to ease the pathway to uses of data for research purposes
- Common Rule Advanced Notice of Proposed Rulemaking (ANPRM) released in July 2011
- Omnibus Rule includes a few provisions:
  - Allow remuneration for transfers of PHI for research (must be reasonable fee based on costs)
  - Allowance of compound authorizations
  - Authorizations no longer have to be study-specific; can have an authorization for future research as long as the description of the future research uses is sufficiently clear that it would be "reasonable for an individual to expect that his/her PHI could be used or disclosed for such future research"

Right to Request Restrictions on Data Sharing with Payors

- Applies to providers
- Mandatory non-disclosure of PHI if requested and
  - Full out-of-pocket payments for particular health services
  - Doesn't meet annual deductible requirements under health plan coverage
- Can't impose all or nothing rules (although if payments bundled, patient must be advised that she must pay for bundle)
- Can disclose information needed to support payment for follow-up care if patient declines to pay out-of-pocket for follow-up
- Must make effort to get appropriate payment from patient if initial mechanism fails (like bounced check)

Notice of Privacy Practices (NPP)

- NPPs must include:
  - statements regarding certain uses and disclosures requiring authorization - e.g., psychotherapy notes (where appropriate), marketing, sales of PHI, right to restrict disclosures to health plans (provider only), and right to be notified of breach; and
  - general statement that all uses and disclosures not described in NPP also require authorization

Omnibus Rule – NPPs must be Revised

- Changes in rule are material
- For plans that post on website, post revised NPP by effective date and in next annual mailing
- If no web site, plans must provide within 60 days of material revision
- For providers, must post and make available upon request; must provide to (and seek acknowledgement from) new patients
- Can send by e-mail if individual agrees

Genetic Information – GINA

- Prohibits genetic discrimination in health insurance and employment
- Rule implements GINA by:
  - Declaring genetic information (defined in GINA) to be PHI
  - Prohibiting most health plans covered by HIPAA from using or disclosing PHI that is genetic information for underwriting
  - Requiring plans to notify beneficiaries about this restriction in the NPP
- Exception for long-term care insurers, who can use genetic information for underwriting

Enforcement Rule

- Enforcement IFR (10/30/09) made changes to the Enforcement Rule that took effect under HITECH as of 2/18/09
- HITECH NPRM (7/14/10) proposed changes to the Enforcement Rule as revised by the IFR
- Omnibus Rule: changes to compliance, investigations and penalties

Enforcement Rule -- BAs, Investigations, Reviews

- Civil monetary penalties (CMPs) can be assessed directly to business associates
- Complaint investigations and compliance reviews
  - Required whenever there is evidence of a possible HIPAA violation due to willful neglect
  - Discretionary in the absence of possible willful neglect
  - Every complaint will be investigated preliminarily
  - Secretary has discretion to move directly to imposition of CMPs without informal resolution

Enforcement – Coordination

- Secretary may disclose PHI to another agency on request
- Coordination of Department of Justice and FTC (http://www.hhs.gov.ocr/enforcement)
- Coordination with State Attorneys General to assist with their direct enforcement

Enforcement - CMPs

- Three tiers of penalties carried over from Enforcement IFR
  - Did not know $100-$50,000
  - Reasonable cause $1000-$50,000
  - Willful neglect corrected $10,000-$50,000
  - Willful neglect not corrected $50,000
- Annual cap $1.5 million per type of violation
- New definition of “Reasonable Cause” to address state of mind: knew it was a violation but without willful neglect
- Definition of “willful neglect” retained: “conscious, intentional failure or reckless indifference”

Enforcement – CMPs – Liability for Agents

- CEs and BAs and subcontractors are liable for HIPAA violations of their agents
- Apply Federal common law – liability of principal for acts of its agents acting within the scope of its agency
- Fact specific determination: did the principal control or have the right to control or direct the agent's conduct in performing a contracted service?
- The manner and method the principal actually controls the service provided is determinative

Enforcement Rule – Considerations for CMPs

- OCR will consider the following:
  - Nature and extent of violation
  - Nature and extent of any physical, financial or reputational harm
  - The covered entity's or business associate's history of prior noncompliance with statute
  - The financial condition of covered entity or business associate
  - Other factors as required for justice
    - Extent of reputational or other harm
    - Time period during which violations occurred
    - Number of individuals affected

Enforcement Rule – Affirmative Defenses to CMPs

- No civil monetary penalties will be assessed for violations occurring prior to February 18, 2011 if violations are punishable under HIPAA's criminal penalties provisions
- For violations occurring after February 18, 2011, civil monetary penalties may not be assessed if a penalty has been imposed under HIPAA's criminal penalties provisions

Enforcement Rule – Affirmative Defenses to CMPs

- For violations occurring prior to February 18, 2009, civil monetary penalties may not be imposed on a covered entity if
  - The covered entity can establish that it did not have knowledge of the violation, and would not even if by exercise of reasonable diligence
  - The violation is due to circumstances that:
    - Make it unreasonable to comply
    - Not due to willful neglect
    - Corrected within 30 days of when learned, or should have learned, of the violation
- Similar standards for violations occurring on or after February 18, 2009, with broadened application to business associates

Next Steps

- Review policies, procedures, forms, and update
- Train staff on new provisions
- Inventory BAs and update BAAs
- Update breach response plan; in particular, update risk assessment and address encryption
- Don’t delay

Thank You for Participating!

Gerry Hinkley
Chair, HIMSS Legal Task Force
Chair, Health Care Industry Team
Pillsbury Winthrop Shaw Pittman LLP
gerry.hinkley@pillsburylaw.com

Deven McGraw
Director, Health Privacy Project
Center for Democracy & Technology
deven@cdt.org

pillsbury

The purpose of this presentation is to inform and comment upon legal and regulatory developments in the health care industry. It is not intended, nor should it be used, as a substitute for specific legal advice inasmuch as legal counsel may only be given in response to inquiries regarding particular situations.