HIPAA Hot Topics

Audits, the Latest on Enforcement and the Impact of Breaches

September 2012
Overview

- HITECH Act
- HIPAA Audit Program: update and initial results
- Recent uptick in HIPAA enforcement actions
- Breach notification: obligations and how to respond
HITECH Act Impact

• Enacted February 17, 2009
• Established a federal breach reporting obligation
• Enhanced enforcement provisions
  – Harsher penalties for HIPAA violations
  – Authorized State Attorneys General to bring civil enforcement actions
• Direct liability for Business Associates
  – Required to comply with certain Privacy and Security Rule standards
• Mandated performance of periodic HIPAA audits
HIPAA Audits

• Originally 150 Covered Entities to be audited
• Latest from OCR: 115 Covered Entities
  – Every Covered Entity and Business Associate is eligible for an audit (but Business Associates to be audited in a later audit wave)
  – OCR to audit a broad range of types and sizes of Covered Entities, including:
    • Health plans of all types
    • Health care clearinghouses
    • Individual and organizational providers
• Initial round of audits complete; full range of audits rolled out by December 2012
How does the audit work?

• Notification from OCR
  – Entities receive letter and request for documentation
  – Broad data request

• Site visit

• Summarize findings and results; identify issues

• Final report submitted
  – How audit was conducted
  – Findings
  – Action the Covered Entity is taking in response to the findings
OCR Findings after First 20 Audits

- **Small covered entities had more significant issues than large entities.**
  - Small covered entities ($50 million or less in revenue) represented 30% of total audited entities but evidenced 66% of the deficiency findings.

- **Health care providers had more problems than plans or clearinghouses.**
  - Providers represented 50% of the total audited entities but were responsible for 81% of the deficiency findings.

- **Security Rule compliance is the larger concern.**
  - 65% of the deficiency findings were related to the Security Rule, followed by the Privacy Rule (26%), and the Breach Notification Rule (9%).
  - OCR indicated that this is partially attributable to more of the audit protocol focusing on security than privacy or breach notification.
Findings Cont’d

• Majority of deficiencies concerning the Privacy Rule involved:
  – Review process for denials of patient access to records
  – Failure to provide appropriate patient access to records
  – Lack of policies and procedures
  – Uses and disclosures of decedent information
  – Disclosures to personal representatives
  – Business associate contracts

• Majority of deficiencies concerning the Security Rule involved:
  – User activity monitoring
  – Contingency planning
  – Authentication/integrity
  – Media reuse and destruction
  – Risk assessment
  – Granting and modifying user access
Audit takeaways

- Not clear there will be more after this project
- Reinforces need to have HIPAA house in order
- Data requests are broad/limited time to respond
- Even if not covered by audits, recommend reviewing existing compliance as if you received a request
Enhanced Enforcement

• OCR has been the “kinder gentler” side of the government
• Recent actions suggest a change in tone
  – Public statements suggest a harsher approach
  – Congress has pushed for more enforcement
  – OCR follow-up to complaints more onerous and less easily resolved
  – Enforcement actions with teeth
Recent OCR Investigations

- *Phoenix Cardiac Surgery* (April 2012): small physician practice fined for lack of HIPAA safeguards
  - small, non-institutional provider (owned by 2 physicians)
  - OCR received a complaint that the provider was placing PHI on a public website for scheduling appointments
  - OCR investigated the practice and determined that group failed to:
    - implement adequate policies and procedures;
    - conduct risk analysis;
    - document HIPAA training of employees; and
    - obtain proper business associate agreements with internet based email and calendar services, etc.
  - resolution agreement and $100,000 penalty imposed
Recent OCR Investigations

• June 2012: first enforcement action against a state agency
  – Alaska Department of Health and Social Services settled for $1.7 million and entered into a corrective action plan to resolve possible violations of the HIPAA Security Rule.
  – Failure to implement security procedures and safeguards

• March 2012: enforcement action resulting from failure to comply with breach response obligations
  – Blue Cross Blue Shield of Tennessee (BCBST) to pay HHS $1.5 million for failure to properly re-evaluate security measures in response to theft of hard drives containing PHI.
Recent OCR Investigations, cont’d.

- Feb. 2011: individual rights violation
  - $4.3 million civil monetary penalty imposed on Cignet Health for violating 41 patients’ individual rights by denying them access to their medical records and failing to comply with OCR’s investigation

- Feb. 2011: harsh penalty for failure to implement and follow procedures
  - Massachusetts General Hospital agreed to pay $1 million to resolve a privacy rule violation when an employee lost the medical records of 192 patients on a subway train
Civil Penalties

- HITECH established a tiered system of penalties
  - Did not know (even with diligence): minimum of $100 per violation
  - Reasonable Cause: minimum of $1,000 per violation
  - Willful Neglect:
    - Organization corrected violation: minimum of $10,000 per violation
    - Organization did not correct violation: minimum $50,000

- For all types: Up to $1,500,000 per year for multiple violations of the same part of HIPAA
Criminal Enforcement

• Criminal penalties can be imposed not only on CEs and BAs but also on individual employees who obtain or disclose PHI without authorization:
  – $50,000 plus one year imprisonment for knowingly violating HIPAA; to
  – $250,000 plus ten years’ imprisonment for doing so with intent to profit by or do harm with the information

• May 2012: Ninth Circuit Court of Appeals rules that knowledge of illegality not needed for criminal conviction under HIPAA

• August 2012: owner of NY medical supply company convicted
  – Defendant stole PHI from nursing homes and submitted false claims to Medicare
New Enforcement Approaches

• State Attorneys General authorized to bring action for HIPAA violations

• January 2010: Connecticut AG first to bring action
  – $250,000 settlement with Health Net for violations of the Security Rule and breach reporting obligation

• February 2012: Minnesota AG brings action against a Business Associate
  – Action against Accretive Health (debt collection agency) for failure to safeguard patients’ PHI
  – Followed up with comprehensive “compliance review” and allegations of illegal billing and collections practice
Enforcement Takeaways

• Again: good time to get your HIPAA house in order
• Expect detailed requests in response to a complaint or breach (copies of policies; copies of training; training logs; copies of most recent risk analysis; updates on actions taken in response to risk analysis, etc.)
• If you have a breach involving more than 500, expect an OCR investigation
• If you have a disgruntled patient, think through possible HIPAA complaints they could file
Breach Notification: What is a Breach

- A breach occurs when PHI is used, disclosed, or accessed in a way that is not permitted by the Privacy Rule and compromises the security or privacy of the PHI.
- Does not include incidents that do not pose a significant risk of harm to the individual.
- If an “inadvertent disclosure” of a patient’s PHI occurs in such a way that the person did not have time to retain the data, and if the data was not shared with anyone else, this would not be a breach.
Breach Notification:

• Covered Entity that discovers a breach of unsecured PHI is required to notify each individual whose PHI was affected by the breach

• A Business Associate that discovers a breach must notify the Covered Entity of the breach
Breach Notification: Unsecured PHI

• “Unsecured PHI” means PHI that is not secured through specific methods determined by HHS
• According to HHS, there are two methods that can be used to secure PHI: (1) Encryption and (2) Destruction
Notification of a Breach

• **Individual notice**
  – First class mail, unless e-mail is preferred
  – If the Covered Entity doesn’t have sufficient contact information for an individual, the breach must be disclosed on the company’s website or published in major print

• **Public notice**
  – If the breach affects fewer than 500 individuals, the Covered Entity must keep a log of the breach and report annually to Secretary
  – If the breach affects more than 500 individuals, the Covered Entity must immediately notify HHS (and in some cases, the media)
Content of Notice

- Notice (to the individual) must include, to the extent possible:
  - Brief description of what happened
  - Description of the type of PHI involved
  - Steps individuals should take to protect themselves
  - Description of what steps the covered entity is taking in response to the breach
  - Contact information for individuals to ask questions and learn more information
Notice to HHS

- Submit notification electronically at OCR website
- Notice includes:
  - Number of individuals affected
  - Contact information for covered entity and business associate, if appropriate
  - Breach information – date(s) of breach and discovery; type of breach; location of breach; PHI involved; brief description of breach; safeguards in place prior to breach
  - Notice of breach and actions taken – date(s) notice provided; media notice; actions taken in response to breach
  - Attestation that the information reported is accurate
Before the Breach

- Training is key: on HIPAA policies and on what to do if you suspect a breach
- Minimum necessary can be your friend
- Encrypt! Encrypt! Encrypt!
- Analyze how data flows and what safeguards you can put in place to reduce human error
After the Breach Incident

- Determine facts (is PHI really involved? Be skeptical of initial “no PHI” answers)
  - May need to engage forensic experts
- Must move quickly to respond
  - Analyze applicable laws (states & HITECH)
  - Draft notices (often time consuming)
  - Time to train call center employees
After the Notices are Sent

- Review file carefully and finish/clarify any incomplete items (incident reports)
- Complete any mitigation steps
- Review and improve impacted policies
- Address any compliance gaps: expect OCR to request policies, disaster recovery plans, etc.
Questions

John E. Kelly, Member
Bass, Berry & Sims PLC

jkelly@bassberry.com
202-827-2953