



## Final Regulations (and Penalties) Related to HIPAA Security Breaches

John L. Barlament  
[JLBarlament@michaelbest.com](mailto:JLBarlament@michaelbest.com)  
[www.michaelbest.com](http://www.michaelbest.com)  
414.225.2793

## New Guidance – and New Worries

---

- American Recovery and Reinvestment Act of 2009 (“ARRA”) modified HIPAA rules
- Applying Security and Privacy Rules to business associates (“BAs”)
- New breach notification rules
- Identifying a “breach”
- Notices to affected individuals
- Notices to media
- Notices to U.S. Department of Health and Human Services (“HHS”)
- Increased penalties

## Applying HIPAA to Business Associates

---

- Commentators had complained of a “gap” in health privacy provisions—i.e., “covered entity” defined somewhat narrowly (health plans main focus here)
- HHS: No authority to go beyond direct regulation of covered entities
- Business associates were “indirectly” covered before, through business associate agreement with covered entity
- BA contract followed many HIPAA rules but not all
- ARRA now directly applies most HIPAA Security Rules (and some Privacy Rules) directly to BA
  - Generally effective February 2010; but, some provisions (e.g., breach rules and penalties) can apply earlier
  - Places BAs in awkward spot—e.g., do not need Security Rule policies and procedures until February 2010—but without those more difficult to identify where electronic PHI is and train workforce on breach rules, which are effective September 2009

## New Breach Notification Rules

---

- “Breach” is the (1) acquisition, access, use or disclosure of protected health information (“PHI”); (2) in a manner not permitted under 45 CFR Section 164, Subpart E; (3) which compromises the security or privacy of the PHI
- Significant differences from statute:
  - Regulations do not incorporate statute’s use of the phrase “accesses, maintains, retains, modifies, records, stores, destroys or otherwise holds, uses or discloses” unsecured PHI
  - Reference to Subpart E
  - New gloss on “compromises” (see below)

## New Breach Notification Rules – Effective Date

---

- Effective for breaches occurring 30 days on and after publication in Federal Register—here, August 24, 2009 and September 23, 2009, respectively
- HHS will use its “enforcement discretion” and not impose penalties until February 22, 2010
  - Unclear if penalties could relate to actions taken (or not taken) between September 23, 2009 – February 21, 2010
- No HHS authority to penalize business associates until February 18, 2010
  - BAs could still have exposure e.g., contract requirements or negligence claims

## “Compromises” PHI – No Harm, No Foul?

---

- “Compromises” PHI defined as a breach that poses “a significant risk of financial, reputation, or other harm to the individual”
- Significant and helpful because covered entity and business associate can now make judgment call about how significant threat is (if not significant, no “breach” and no reporting required)
  - Tip: Health plan may want to have BA report everything then have plan decide what is “significant”
- Consider who impermissibly used PHI or to whom information was impermissibly disclosed when evaluating risk of harm to individuals
- Plan “must” document its risk assessment so it can demonstrate, if necessary, why no breach notice needed

## “Compromises” PHI

---

- Look at nature of PHI was disclosed
- Merely name of individual and fact of plan participation could be Privacy Rule breach but no harm
- If types of treatment revealed or info could lead to identity theft (e.g., social security number, account number or mother’s maiden name), then “higher likelihood” of harm
- Recognize that many types of health details (not just sexually transmitted diseases) can be sensitive, especially given risk of employment discrimination

## “Compromises” PHI -- Examples

---

- Group health plan is coordinating benefits with another HIPAA-covered plan. PHI of Joe A. Smith is shared with other plan—but coordination really involved Joe B. Smith. Fact that other plan is HIPAA-covered means “may be less risk of harm” to Joe A. Smith, therefore breach less likely
- Appeal information is redacted and provided to health plan appeals committee. Information is not collected by committee and information is misplaced and found by someone not on committee. Possibly no “breach” if redacted info is de-identified information or if info does not create significant threat

## “Compromises” PHI -- Examples

---

- Preamble: If can obtain “satisfactory assurance” from accidental recipient that PHI will not be further used or disclosed (e.g., through confidentiality agreement or similar means) or will be destroyed, less risk
  - Still have duty to mitigate improper uses or disclosures
- What if PHI is returned or found? E.g., laptop is lost or stolen, then found or returned a few days later. If “forensic analysis” of computer shows PHI was not opened, altered, transferred or otherwise compromised, may not be significant risk
  - Cannot delay breach notification in hope computer will be recovered

## Four Exceptions to “Breach”

---

- Breach of Secured PHI
- Unintentional acquisition, access or use of PHI by employee or individual acting under authority of plan or business associate (“BA”)
- Inadvertent disclosure of PHI from one person authorized to access PHI at a plan or BA to another person authorized to access PHI at the plan or BA
- Unauthorized disclosures in which unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information

## Secured PHI / Unsecured PHI (Exception #1)

---

- “Unsecured PHI”—PHI not rendered unusable, unreadable or indecipherable to unauthorized individuals through technology or methodology approved by HHS
  - Includes PHI in any form (electronic, paper, oral)
  - 4/17/09 HHS guidance and new regulations “safe harbor” for data: in motion (e.g., moving through a network); at rest (e.g., in a database or flash drive); in use (e.g., data in process of being created, retrieved, updated or deleted); disposed (e.g., discarded paper records or recycled electronic media).
    - Encryption (NIST approved; keys “should” be separate from data)
    - Destruction (shredded or purged)
  - Access controls, firewalls, etc. do not make electronic data “secured”
  - Redaction of paper documents does not make them “secured”

## Unintentional Acquisition (Exception #2)

---

- Unintentional acquisition, access or use of PHI by workforce member or person acting under authority of plan or BA if acquisition, access or use in good faith and within scope of authority and does not result in further use or disclosure in manner not permitted under 45 CFR Section 164 Part E
  - “Workforce member” includes employees, volunteers, others under control of plan
  - BA can be acting “under authority” of plan
  - E.g., billing employee receives and opens email containing PHI about plan participant which fellow employee accidentally sent. Billing employee notices he is not intended recipient, alerts fellow employee of mis-directed email then deletes it.

## Inadvertent Disclosures (Exception #3)

---

- Inadvertent disclosure by a person who is authorized to access PHI at a plan or BA to another person authorized to access PHI at the same plan or BA (or organized health care arrangement in which the plan participates), if the PHI received is not further used or disclosed in a manner violating 45 CFR Section 164, Part E
  - E.g., appeals committee member shares PHI of plan participant with another committee member, thinking the participant had appealed a claim. In fact, it was a different participant who had appealed the claim. Recipient member does not further use or disclose the PHI.

## No Retaining (Exception #4)

---

- Disclosure of PHI where plan or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to “retain” PHI
  - E.g., plan sends a number of EOBs to wrong individuals. Some EOBs are returned by post office, unopened, as undeliverable. Plan can conclude improper addressee could not have retained them. EOBs not returned should be treated as potential breaches.
  - Does “retain” refer to physically retaining it—e.g., stole paper medical record? Or mentally retaining it—e.g., remember co-worker’s situation? Preamble seems to indicate either can apply (in example, nurse gives patient someone else’s medical record; if patient could not “read” the information, no breach)

## “Breach” Identification -- Summary

---

- 1. Plan and BA must determine whether there was an impermissible use or disclosure of PHI under the Subpart E
- 2. Plan or BA must determine, and document, whether the impermissible use or disclosure compromises the security or privacy of the PHI
- 3. Plan or BA should determine if an exception applies (e.g., inadvertent disclosure)

## Polling Question #1

---

- In the past year, has your organization had an event that would qualify as a “breach” under this definition?
- Yes
- No
- Not sure

## Breach Rules—What Happens if Breach Occurs

---

- Scope of responsibility is different for plan versus BA
- BA: After breach is “discovered” report data to plan within time allowed by BA agreement
  - BA need not report breaches to affected individuals; presumably could do so per contract
- Plan: After breach is “discovered” must notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed as a result of the breach
  - Media notice also possible
  - HHS notice required

## “Discovering” a Breach

---

- “Discovered” = first day on which breach is known or should reasonably have been known by covered entity or BA if they had exercised reasonable diligence
- Plan and BA are deemed to have knowledge of workforce members (other than person committing breach) and any agents
  - Agency determined in accordance with federal common law of agency—appears to be somewhat ill-defined
  - Appears BA will often be “agent” of plan
  - In general, very broad reach (e.g., agent / subcontractor of BA will have knowledge attributed to BA; then apparently attributed to plan)
- What if breaching employee never tells anyone else? A breach but never “discovered” therefore no reporting obligation of plan or BA
  - Can lead to other claims—e.g., negligence; inadequate training, etc.

## Notice to Individuals

---

- Notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed as result of breach
  - E.g., hacker breaks into health plan's computer system; potentially every record of all participants accessed; may need to notify every participant of breach unless forensics indicates no access
- Tip: Rules likely put a premium on knowing where PHI is and having system in place to monitor access to PHI
- If business associate discovers breach, BA notifies covered entity of breach (time not specified by regulations; check BA agreement)
- BA notice to covered entity must identify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired or disclosed during
  - Tip: BA should create process and procedure to gather and communicate

## Individual Notice

---

- Plan must make notification without “unreasonable delay”, no later than 60 calendar days of breach discovery
  - 60 days is outer limit; can be unreasonable in some situations
  - Can be in multiple mailings as more details are discovered
  - 60 days begins when breach is first known, not when investigation of incident is complete (even if initially unclear whether it is a breach)
  - If initially thought breach but then discover no breach (e.g., lost laptop one day but find it next and no access in between) then nothing to report
- Burden of proof on covered entity / BA to show timeliness, including evidence demonstrating necessity of delay

## Individual Notice

---

- Written notice by first-class mail to individual at last known address or, if specified by individual, email
  - Notify next of kin or personal representative if plan has information
- If insufficient or out of date contact info so direct notice precluded, notify by “substitute form”
  - If less than 10 individuals, written notice, telephone or other means
  - If 10 or more individuals, conspicuous posting on covered entity’s web site for 90+ days or “conspicuous” notice in “major” print or broadcast media, which must include a toll-free phone number so individual can learn if unsecured PHI was breached
    - Some web page rules (e.g., be on “home page” or provide prominent hyperlink)
    - Any need to publicize fact that web site exists? Should plan set up web site now in anticipation of future breaches?

## Individual Notice

---

- “Major” print and media – apparently facts and circumstances test
  - Depends on geographic area where individuals affected by breach likely reside
  - E.g., if rural, local newspaper ok; if metropolitan area, newspaper covering entire area or state ok; if multiple regions or states, may need multiple media; daily newspaper of specialized interest (e.g., sport, politics) not “prominent” (and presumably not “major”)
  - “Conspicuous” – no guidance on where to place notice; give “thought” to “location and duration” of notice
- If urgency because of possible imminent misuse, can notify by telephone or other means in addition to written means (telephone notice not substitute for written notice)
  - No guidance on what is “urgent”

## Individual Notice – Must Include....

---

- Brief description of what happened, in plain language, including date of breach and date of discovery of breach
  - No specific obligation for other formats (Braille, large print, audio, etc.)
- Types of unsecured PHI involved (e.g., social security number, full name, date of birth, home address, account number, diagnosis)
  - Do not list actual PHI breached
- Steps individuals should take to protect themselves from potential harm
  - E.g., call credit card company or credit monitoring services
- What plan is doing to investigate breach, mitigate harm and protect against further breaches
  - E.g., filed police report, hired consultants
- Contact procedures for individuals to ask questions or learn additional information
  - Must include toll-free phone number, email address, web site or postal address

## Media Notice

---

- Major breach: Notice must be provided to “prominent” media outlets in state or jurisdiction if unsecured PHI of more than 500 residents of state or “jurisdiction” is or is reasonably believed to have been, accessed, acquired or disclosed during breach
  - Presumably “major” media similar to “prominent” media
  - Media notice rules apply in addition to individual notices
  - “Jurisdiction” smaller than state (e.g., county, city, town)
  - If total breach is 600 individuals, 200 in Virginia, 200 in Maryland and 200 in Wisconsin, the breach is not major (because did not affect 500 residents of any one state or jurisdiction)
  - Similar rule for BAs: If 800 affected by breach of TPA’s computers, but 450 are participants of 1 plan and 350 participants in other plan, not major breach

## HHS Notice

---

- If breach of 500+ individuals, provide notice to HHS within time send notice to affected individual
  - Relief—statute calls for “immediate” HHS notification (FTC rules call for 10 day notice)
  - Beware shifting calculations (e.g., think 450 affected; after month of investigating, find 100 more affected)
- If breach less than 500 individuals, maintain log of breach and annually submit to HHS within 60 days of end of each calendar year
  - Likely will require new forms and procedures to document affected individuals
  - HHS web site will include details on how to submit information
  - Appears breaches are not added together (e.g., 6 breaches of 100 individuals falls into yearly notice, not immediate notice)—but can be tough to determine what is the “breach”

## HHS Notice

---

- HHS will identify on its website covered entity's breach if unsecured PHI of more than 500 individuals is acquired or disclose
- HHS reports to Congress annually on these breaches
- First report for calendar year 2009 due by approximately March 1, 2010
  - Will only relate to breaches occurring on or after September 23, 2009

## Business Associate Notification

---

- Business associate shall notify plan of breach of unsecured PHI after BA discovers breach
- Same rule as for plans regarding when breach is “discovered”
  - Agent / subcontractor’s knowledge likely attributed to BA
- BA must provide notice to plan without unreasonable delay, in no event later than 60 days after breach discovered
  - Big change--direct statutory requirement, not just contract violation if BA fails to take action
- BA provides list of each individual whose PHI was breached and any other information plan needs to send out notice to individuals (e.g., what happened and when)

## Polling Question #2

---

- For business associates only: Do you have privacy- or security-related policies and procedures in place today?
- Yes
- No
- Not sure

## Other Regulation Changes

---

- Law enforcement delay to notice (if verbal, maximum 30 days and must be documented; if written, time period specified)
- Burden of proof on plan or BA to prove all notifications provided
- Plan workforce must be trained on new rules
- Complaint process must include ability to complain about this area
  - Does this require updating a notice of privacy practices?
- Sanctions apply to failures to comply with new rules
- No retaliation / waiver / intimidating acts

## What is Not Addressed

---

- HHS will issue more guidance on most effective and appropriate technical safeguards for use in carrying out Security Standards
- HHS will designate an individual in each regional office to offer guidance and education to covered entities, BAs and individuals on privacy and security rights and responsibilities (August 2009)
- HHS will conduct education initiatives to educate individuals about uses of PHI (February 2010)
- Whether BAs are subject to all or only a few Privacy Rule requirements

## What is Not Addressed

---

- New restriction request rules
- New guidance on “minimum necessary”
- New disclosure accounting and access rules for electronic health records (“EHRs”)
- Prohibiting sale of PHI

## Increased Penalties and Enforcement

---

- Penalties must be imposed if HIPAA violation due to “willful neglect” (and HHS required to investigate) (February 2011)
- Funds from imposed penalties are transferred to Office for Civil Rights (part of HHS) to be used for enforcing HIPAA
- By August 2010 HHS proposal on how individuals harmed can recover a percentage of any civil monetary penalty or settlement (HHS to issue regulations by February 2012)
- State attorney generals can sue to enforce and seek attorney fees
- HHS audits now required

## Increased Penalties and Enforcement

---

- Currently, penalties vary somewhat, but general penalty is \$100 per HIPAA violation (cap of \$25,000 for multiple violations in same year)
- Under ARRA, minimum \$100 if did not know of violation and would not have known even with reasonable diligence (cap of \$50K per violation, \$1.5M total)
- If reasonable cause and not willful neglect, minimum \$1,000 penalty (cap of \$50K per violation, \$1.5M total)
- If willful neglect but corrected, minimum \$10,000 penalty (cap of \$50K per violation, \$1.5M total)
- If willful neglect and not corrected, minimum \$50,000 penalty (cap of \$1.5M)
- Effective February 2009

## Practical Steps

---

- Identify and update all BA agreements
- Modify policies and procedures
- Update handbook / sanction policy if needed
- Train workforce



## Questions and Answers

---

- Any questions?
- Thank you for attending
- **A3446709**

John L. Barlament  
Michael Best & Friedrich LLP  
100 E. Wisconsin Avenue  
Suite 3300  
Milwaukee, WI 53202  
[JLBarlament@michaelbest.com](mailto:JLBarlament@michaelbest.com)