Quarles & Brady LLP

October 17, 2014

Birds of a Feather Comply Together:
An Analysis of the Relationship Between Covered Entities and Business Associates When Navigating the HIPAA Breach Notification Rules

Jennifer L. Rathburn
Jennifer J. Hennessy

hipaacow.org

1

Agenda

- Breach Statistics and Costs
- Security Breach Investigation Steps
  - Analysis of the low probability of compromise standard
- Notification in Event of a Breach
- Downstream Liability and Other BA Considerations
- Practical Tips

2

Breach Costs

- Investigations and incident response
- Containment/Remediation
- Legal fees
- Loss of competitive advantage
- Lost sales, revenues & profits
- Reputational harm
- 3rd party claims for negligence and breach of contract & potential class action suits
- Termination/Cancellation of K or relationship
- Renegotiation of confidentiality & indemnification terms

3

Cost of Data Breach Study: US*

United States Highest Cost!!!

- The average cost per compromised record has increased
  - 2013 = $201 *But health care ($359), education ($294), financial ($206) industries higher
  - 2012 = $188
- The average total expense to an organization (notification, maintaining call centers, legal, investigative and administrative expenses) has increased
  - 2013 = $5.85M
  - 2012 = $5.4M
- Lost business costs (abnormal turnover, reputational losses, diminished goodwill) have increased.
  - 2013 = $3.32M
  - 2012 = $3.03M
- Malicious/criminal attacks (44%), human error (31%), and system glitches (25%) are reported as the main causes of data breaches

* Ponemon Institute© Research Report - 2014

4

But wait, there's more …

Certain factors reduce the overall cost of a breach per record

- Strong security posture ($14)
- Incident response plan ($12)
- Business continuity plan ($8)
- CISO with enterprise–wide responsibility ($6)

BUT

- Organizations that responded or notified customers too quickly without a thorough assessment of the breach paid an average of **$10** more per record!
- Breaches caused by lost or stolen devices increased the cost of a data breach by as much as **$16** per record

Probability it will happen to your company in the next 24 months?

- A material data breach of over 10,000 records is approximately 22%.

* Ponemon Institute© Research Report - 2014

5

Security Breach Investigation Steps

1. Determine whether there has been an **impermissible acquisition, access, use or disclosure** of PHI in violation of the Privacy Rule
2. Determine if the PHI is **unsecured**
3. Evaluate whether the incident **falls under one of the exceptions** to the notification obligations
4. Conduct a **risk assessment** to determine whether the impermissible use or disclosure poses a **low probability of compromise** to the PHI
5. **Resist** the urge to automatically assume notification is required

6

What Is Not a Reportable Breach?

- Violations of the HIPAA Security Rule and certain violations of the HIPAA Privacy Rule
  - E.g., CE's failure to provide Notice of Privacy Practices
- Use or disclosure of de-identified information
- Impermissible use or disclosure of PHI that is **incident to** an otherwise permissible use or disclosure, and
  - Occurs despite reasonable safeguards and proper minimum necessary procedures

7

Unsecured PHI

- Breach notification obligations under the HITECH Act only apply to breaches involving "**Unsecured PHI**"
- The HITECH Act defines "**Unsecured PHI**" as PHI that is not secured through the use of a technology or methodology that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals
  - Generally, secure means encrypted or properly destroyed consistent with NIST
- BAAs require BA to encrypt/destroy data in accordance with NIST?

8

Importance of Encryption

- Per OCR, 60% of breaches on "Wall of Shame" caused by theft and loss
- All would have been prevented by encryption!

9

Exceptions

- **Unintentional** acquisition, access, or use of PHI by a workforce member or person acting under the authority of a CE or BA
  - If such unintentional activity was done in good faith, within the course and scope of employment or other professional relationship, and
  - Does not result in further use or disclosure in violation of the Privacy Rule
- Does not cover snooping employees

10

Exceptions, continued

- **Inadvertent** disclosure of PHI from one person with authority to access PHI at a CE or a BA to another person who also has authority to access PHI
  - If such inadvertent recipient is part of the same CE, BA or Organized Health Care Arrangement as the individual who made the inadvertent disclosure
  - Provided the recipient does not further use or disclose the information in violation of the Privacy Rule

11

Exceptions, continued

- **Unauthorized** disclosures in which the person to whom PHI is disclosed would not reasonably have been able to retain the information
  - Based on "good faith" belief by disclosing CE or BA
    - E.g., handing the wrong medical records to a patient and immediately taking them back
    - E.g., sending explanation of benefits (EOB) to wrong individual if EOB is returned by post office, unopened, as undeliverable

12

Risk Assessment

- Notification required unless a low probability that the PHI has been compromised
  - Also, **presumption** that impermissible use or disclosure is a breach!
- Focus is on the risk the PHI was compromised (previously the focus was on the risk of harm to the individual)
- Who is required to do risk assessment?
  - Should BA complete risk assessment? Turn over to CE?

13

Four Factors to Consider

1. **Nature and extent of the PHI**, including types of identifiers and likelihood of re-identification
2. **Unauthorized person** who used the PHI or to whom the PHI was disclosed
3. Whether the PHI **actually acquired or viewed**
4. Extent the risk to the PHI has been **mitigated**

14

Focus on Factor 4: Extent the Risk Was Mitigated

- Quickly mitigating any risk to PHI that was improperly used or disclosed may lower the risk that the use or disclosure will constitute a breach
  - E.g., receive assurances (e.g., a confidentiality agreement) from recipient that the PHI will be destroyed or will not be further used or disclosed
- Consider extent and efficacy of the mitigation
  - Assurances from employee, affiliated entity, CE, BA, or sub-BA vs. assurances from other third parties
- Consider BA's obligation to mitigate

15

Complete Risk Assessment

- Analyze four factors, plus any other relevant factors
- Evaluate overall probability that PHI has been compromised
- Risk assessment must be thorough, completed in good faith, and conclusions must be reasonable
- Must be documented in writing
- **Notification required if risk assessment fails to show low probability that PHI has been compromised**

16

Complete Risk Assessment, continued

- If notice is provided, no risk assessment is necessary
- OCR says it will issue guidance on performing risk assessments for frequently occurring scenarios

17

Burden of Proof

CE or BA has burden of proof for showing why breach notification was not required!

18

BA's Notification Obligations

- BAs must notify CEs without unreasonable delay and in no case later than 60 days after BA discovers breach (no delay for investigation)
- Considered to have been discovered when workforce member (other than the person who committed the breach) or other **agent** finds out
- If BA is an agent of CE, the 60-day clock starts running the day the BA "discovers" the breach
- Agency relationship determined by principles of federal common law

19

BA as Agent of CE

- Fact specific inquiry
- Totality of circumstances involved in relationship between CE and BA
- **Four factors to consider:**
  - Time, place, and purpose of BA's conduct
  - Whether BA engaged in a course of conduct subject to CE's control
  - Whether BA's conduct is commonly done by a BA to accomplish the service performed on behalf of a CE
  - Whether the CE reasonably expected that BA would engage in the conduct in question

20

BA as Agent of CE, continued

- **Essential factor:** CE's authority to control BA's conduct in performing service on behalf of the CE
  - Terms of BAA
    - Authority of a CE to give interim instructions or directions
    - If CE has to amend BAA or sue for breach of contract, BA probably not an agent
  - Type of service and skill required to perform the BA service
    - BA hired to provide de-identification for small provider likely not an agent
    - BA hired to provide services CE cannot legally perform (e.g., accreditation) likely not an agent

21

BA as Agent of CE, continued

- BA can be an agent:
  - Despite the fact that CE does not retain the right or authority to control every aspect of its BA's activities
  - Even if a CE does not exercise the right of control but evidence exists that it holds the authority to exercise that right
  - Even if a CE and its BA are separated by physical distance (e.g., if a CE and BA are located in different countries)
- The term used (agent or independent contractor) will not determine whether BA is an agent

22

Downstream Liability

- CEs are liable for breaches of BAs who are their agents!
- BAs are liable for breaches of Sub-BAs who are their agents!

23

CE Notification Requirements

- Upon determination that a reportable breach has occurred, the CE must provide notification
  - Can delegate to BA when appropriate
- CEs must timely notify:
  - Individuals in writing (limited exceptions)
  - Media if 500 or more individuals have their unsecured PHI breached in the same State or jurisdiction
  - HHS Secretary

24

Notification Timing

- CEs to notify without unreasonable delay, and in no case later than 60 calendar days from "discovery"
  - Actual discovery or when should have discovered using **reasonable diligence**
    - Must take reasonable steps to learn of breaches
    - Must investigate if indications of a breach
  - CEs are not liable for failure to provide notice where the CE did not know or have reason to know of the breach
- No delay for investigation

25

Other Considerations

- Wisconsin Law
- Section 5 of the FTC Act
- Payment Card Industry (PCI) Data Security Standards
- International Breach Laws

26

Additional Reporting Obligations for BAs

- Security Incidents
- Uses and Disclosures in violation of the terms of the BAA
- Even if Security Incident/Use or Disclosure does not constitute a breach!!!

27

Required to Report *Suspected* Breach?

- BAs should review their BAAs to determine if BA is required to report *suspected* breaches to the CE

28

Recent Trends in BAAs

- Audits, security risk analysis, and questionnaires
  - Meet with BA's IT folks
- Access to BA's policies and procedures
  - Including BA training log
- Indemnification
  - Violations of HIPAA
  - Breach of BAA
  - Costs of a breach of unsecured PHI

29

Recent Trends in BAAs, continued

- Insurance
- Prohibition on offshore work
- No subcontractors unless approved by CE
- Require BA to return or destroy information/cost of destruction
- Prohibit comingling of CE's PHI with PHI from other accounts

30

Practical Tips

- Focus on BAs:
  - With access to a lot of PHI
  - With access to sensitive PHI
  - Handling critical functions for the CE
- BAs are extension of CE
  - Especially important when OCR picks up audits of BAs
- Determine BAA terms your entity will:
  - Insist be included in all BAAs vs. Prefer be included in BAAs (but will concede on)

31

Note on Audits

- Unsure when audits will commence due to budget constraints
- But when they do, audits will result in compliance reviews
- Meaning OCR intends audits to be enforcement tools
- OCR intends to issue financial penalties from audits initiated by OCR if violations are discovered, even where there has been no breach of unsecured PHI

32

Audits, continued

- CEs audited should inform BAs because they too may be audited
- Get documents in order
  - All documentation must be current as of the date of the request by the OCR
  - Auditors cannot ask for clarification or additional information so documents must accurately reflect practices

33

Penalties

- OCR may impose a Civil Monetary Penalty (CMP) for failure to comply with the breach notification rule
- OCR has discretion to work with CE to achieve voluntary compliance through informal resolution, **except in cases of willful neglect**
- Don't forget! OCR may still impose a CMP for the underlying Privacy Rule violation, even when all breach notification requirements were met

Quarles & Brady LLP

Jennifer L. Rathburn
Quarles & Brady LLP
411 E. Wisconsin Avenue
Milwaukee, WI 53202-4497
(414) 277-5256
jennifer.rathburn@quarles.com

Jennifer J. Hennessy
Quarles & Brady LLP
33 E. Main Street
Madison, WI 53703-3095
(608) 283-2405
jennifer.hennessy@quarles.com