One Year After the HIPAA Omnibus Rule: Lessons Learned in Breach Notification

HCCA Compliance Institute
April 22, 2015
Adam H. Greene, JD, MPH
Partner
Davis Wright Tremaine
Doug Pollack
Chief Strategy Officer
ID Experts

Agenda

- Basics of HIPAA Breach Notification Rule
- Interim Final Breach Notification Rule
- HIPAA Omnibus Rule Changes
- Operationalizing Incident Response Management & Breach Notification
- Lessons Learned from Breach Data and Settlements
- Case Studies
Basics of HIPAA Breach Notification Rule

- Business Associate
- Covered Entity
- Affected Individuals

(if > 500 in state/jurisdiction)
Timing of Breach Notification

- **Business associate (BA) to covered entity (CE):**
  - Without unreasonable delay, no later than 60 days

- **CE’s deadlines begin upon:**
  - Receipt of notice from BA if BA is *not* agent of CE
  - BA’s discovery if BA *is* agent of CE

- **Agency depends on if CE controls BA beyond strict terms of the contract (e.g., can provide interim instructions)**

Timing of Breach Notification

- **CE to affected individuals:**
  - Without unreasonable delay, no later than 60 days

- **CE to local media (if > 500 individuals in state/jurisdiction):**
  - Without unreasonable delay, no later than 60 days

- **CE to Office for Civil Rights (OCR):**
  - If ≥ 500 individuals, without unreasonable delay, no later than 60 days
  - If < 500 individuals, within 60 days of end of calendar year of discovery
“Unsecured” Protected Health Information

Protected health information (PHI) is “unsecured” if not rendered unusable, unreadable, or indecipherable through:

- Appropriate destruction
- Encryption in accordance with National Institute of Standards and Technology guidance (and encryption key is not compromised)

Three Statutory Exceptions

1. Unintentional acquisition, access, or use
   - Member of the workforce
   - Good faith
   - Within the scope of authority
   - No further use or disclosure in violation of Privacy Rule
Three Statutory Exceptions

2. Inadvertent disclosure
   - By a person authorized to access the PHI
   - To another person authorized to access PHI at the same facility, business associate, or participant in the organized health care arrangement
   - No further use or disclosure in violation of Privacy Rule

3. No retention
   - Good faith belief
   - Unauthorized person would not reasonably have been able to retain the PHI
Risk of Harm Standard:

For purposes of [the definition of “breach”], *compromises the security or privacy of the* [PHI] *means poses a significant risk of financial, reputational, or other harm to the individual.*
**Interim Final Breach Notification Rule**

*Burden of proof.* In the event of a use or disclosure in violation of [the Privacy Rule], the covered entity or business associate, as applicable, shall have the burden of demonstrating that **all notifications were made** as required by this subpart or that the use or disclosure **did not constitute a breach**, as defined at § 164.402.

**Life Under the Harm Standard**
“We recognize that some persons may have interpreted the risk of harm standard in the interim final rule as setting a much higher threshold for breach notification than we intended to set.”
“[T]o further ensure that this provision is applied uniformly and objectively by [CEs] and [BAs], we have removed the harm standard and modified the risk assessment to focus more objectively on the risk that the [PHI] has been compromised.”

“For example, if a [CE] misdirects a fax containing [PHI] to the wrong physician practice, and upon receipt, the receiving physician calls the covered entity to say he has received the fax in error and has destroyed it, the [CE] may be able to demonstrate after performing a risk assessment that there is a low risk that the [PHI]....”
“...Although this scenario does not fit into any of the statutory or regulatory exceptions, we believe that, like the exceptions to breach, notification should not be required if the [CE] demonstrates a low probability that the data has been compromised.”

[A]n acquisition, access, use, or disclosure of [PHI] in a manner not permitted under [the Privacy Rule] is presumed to be a breach unless the [CE] or [BA], as applicable, demonstrates that there is a low probability that the [PHI] has been compromised based on a risk assessment of at least the following factors:
HIPAA Omnibus Rule

No one defined “compromise”!

HIPAA Omnibus Rule

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
   - Does the information create identity theft risk?
   - Is there detailed clinical information?
   - Can the information be used to adversely effect the individual or for the recipient’s gain?
   - List of patient names, addresses, and hospital IDs likely would be a breach.
   - For list of only dates and diagnoses, what is capability of re-identification?
2. The unauthorized person who used the protected health information or to whom the disclosure was made.
   - Recipient subject to HIPAA, Privacy Act, FISMA, or other legal obligations to protect the information?
   - If not readily identifiable, what is recipient’s ability to re-identify the information?

3. Whether the PHI was actually acquired or viewed.
   - Can forensics demonstrate no access?
   - Does actions (e.g., call from recipient indicating that information was received in error) indicate actual viewing?
4. The extent to which the risk to the PHI has been mitigated.
   – Obtaining the recipient’s satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed.
   – Consider credibility of recipient’s statements.

HIPAA Omnibus Rule

Other Factors?
Operationalizing Breach Notification

Why Operationalize?

- High Incident frequency levels
- Requires collaboration across functions
- Within complex regulatory environment
- With the burden of proof on you
- And aggressive enforcement for non-compliance
Learning from Others

“Forward-thinking companies are using governance as the masthead for risk management across privacy, risk, security, IT, and compliance. Allocation of resources is considered on an enterprise level, not just within a particular domain. In this way, multiple business problems can be solved with one investment.”

Jason Taule, CSO/CPO, FEi Systems

“We constantly reinforce the responsibility our workforce members have to report a security event. We prefer that they ‘over-report’ than have a potential problem slip by.”

— Dee Chouinard, Privacy Officer, Harvard Pilgrim Healthcare

“CSOs, particularly new ones, need the people and technologies to identify and address the security risks in their organization. If they had these resources, they’d be surprised at the number of threats to their systems and data.”

— Ken Patterson, CSO, Harvard Pilgrim Healthcare

“A true measure to success for us is mitigation and corrective action. We track reoccurring issues in the software with customized fields of root causes that identify people, process systems, and root-cause departments—in essence, how an incident happened. We can see patterns of issues, and refresh our training and education in these problem areas.”

“Companies need a good layered defense strategy, but that by itself is not sufficient. They must also have great detection and response capabilities. If the bad guys want you bad enough then you will be breached, and if you don’t detect and respond fast enough you will be another victim in the headlines.”

By the Numbers

63,437
ANNUAL SECURITY INCIDENTS

277
HIPAA BREACHES 500 OR MORE RECORDS

30%
PHI BREACHES INVOLVING A BUSINESS ASSOCIATE

2%
INCIDENTS THAT ARE BREACHES

90
APPROX NUMBER OF SMALL HIPAA BREACHES FOR EVERY LARGER ONE

8,899,610
PATIENT RECORDS BREACHED IN 2014 (500 OR MORE RECORD BREACHES)

12014 Data Breach Investigations Report (DBIR), Verizon, 2OCR Website, 3OCR Presentation, 4OCR 2014 Redspin Breach Report
New Ponemon Study Key Findings

Ponemon Institute, Fifth Annual Study on Privacy & Security of Healthcare Data, to-be-released May, 2015

- Data breaches of PHI continue to rise
  - Covered entities having more and larger data breaches (40% > 5 reported breaches)
  - 59% of business associates had at least one breach
  - Over 50% of all organizations have little or no confidence in their ability to detect all breaches

www.idexpertscorp.com/ponemon2015

Criminals are targeting health data

- Criminal attacks up 125% over 5 years
- Almost 60% of healthcare data breaches are malicious
- But 70% of covered entities most concerned about employee negligence

www.idexpertscorp.com/ponemon2015
New Ponemon Study Key Findings

- **Security incidents are ubiquitous**
  - 100% of respondents experience electronic security incidents
  - But one-third of respondents don’t have an incident response plan
  - 40% of covered entities and 42% of business associates *don’t* perform a compliant risk assessment (per Omnibus Rule) for security incidents

  www.idexpertscorp.com/ponemon2015

New Ponemon Study Key Findings

- **Threat of medical identity theft growing**
  - Up 20% this past year
  - But 65% of covered entities and 63% of business associates *don’t* offer any protection or monitoring services to breached individuals
  - Medical ID theft almost doubled over 5 years from 1.4MM to 2.3MM adult American victims

  www.idexpertscorp.com/ponemon2015
“Operationalizing” All About Process

Incident Response Process

Electronic (Digital)
- Security Event
  - Detected or Reported
- Security Incident
  - Root Cause Analysis
- Corrective Action
- Security Remediation
- Document & Close

Analog (e.g. Paper or Visual)
- Event
- Incident
  - Privacy Incident
    - (Typically) Reported
- Root Cause Analysis
- Corrective Action
- Privacy Remediation
- Document & Close

Security
- Breach
  - Large or Malicious
    - Convene Breach Response Team
    - Implement Breach Response Plan
  - Small & Non-Malicious
    - Notify Breach
    - Standard Notification

Risk
- Legal Compliance

Document Assessment

Privacy

dwt.com 36 idexpertscorp.com
The Incident Risk Assessment

- Point of convergence between security, privacy and compliance
- The “gate” between incident management and breach response management
- Our “approach” is automated by intelligent software
- Uses modeling to assist in determining if an incident is a breach under HIPAA and state regulations

The RADAR® Way

- Incident information capture
  - Data affected in incident
  - Nature & specifics of incident
  - Jurisdictions of incident (fed/states)

Factor weightings based on:
- HIPAA/HITECH Omnibus Rule
- State Breach Notification Law Rules

Breach Guidance Engine

Is this a breach under HIPAA/Omnibus?

Is this a breach under affected state(s)?
Benefits of This Approach

- Quantitative model gives consistent and repeatable results
- Significantly reduces time for incident risk assessment
- Spans federal and state laws along with their complexity

Using Incident Data to Reduce Risks

- Using a methodology such as the one in RADAR, you capture valuable metadata on every incident
- Incident metadata can direct you to areas with privacy/security vulnerabilities and weaknesses
- Thereby improving your overall risk profile and ability to reduce privacy breaches
Example

Keys to Operationalize Incidents

- Have a repeatable methodology
- Have clear roles and responsibilities for incident capture, risk assessment, remediation, notification
- Maintain accessible documentation of incidents and decisions
- Automate whatever is possible to automate to remove inconsistency
Lessons Learned from Breach Data and Settlements

Incident Volume by Industry\(^1\)
Proportion %

\[24\%\]
\[32\%\]
\[33\%\]
\[11\%\]

\(^1\)ID Experts Data Analysis
Paper Incidents a Majority

- Insurance/Finance: 46%
- Providers (Hospitals): 26%
- Pharmacy: 8%

*ID Experts Data Analysis*

Reported Breaches Involving 500 or More Individuals
Cause of Breach by Number of Incidents (as of 2/15/15)

- Theft, 598, 53%
- Unauthorized Access/Disclosure, 205, 18%
- Other, 99, 9%
- Loss, 94, 8%
- Hacking/IT Incident, 84, 7%
- Improper Disposal, 43, 4%
- Unknown, 13, 1%
- Improper Disposal, 43, 4%
- No Cause Listed in HHS Data, 3, 0%

Source: www.hhs.gov/ocr
Reported Breaches Involving 500 or More Individuals
Cause of Breach by Number of Individuals (as of 2/15/15)

No Cause Listed in HHS Data, 16,163, 0%
Improper Disposal, 685,214, 2%
Other, 1,247,156, 3%
Unknown, 2,084,987, 5%
Hacking/IT Incident, 3,404,632, 8%
Unauthorized Access/Disclosure, 4,509,523, 11%
Loss, 7,352,646, 18%

Source: www.hhs.gov/ocr

Reported Breaches Involving 500 or More Individuals
Type of Media by Number of Incidents (as of 2/15/15)

EMR, 38, 4%
Laptop, 240, 21%
Other Portable Electronic Device, 300, 26%
Desktop Computer, 128, 11%
Other, 160, 14%

Source: www.hhs.gov/ocr
Reported Breaches Involving 500 or More Individuals
Type of Media by Number of Individuals (as of 2/15/15)

- Network Server, 10,159,470, 25%
- Desktop Computer, 7,153,721, 17%
- Other Portable Electronic Device, 1,504,762, 13%
- Paper/Films, 1,859,303, 5%
- EMR, 1,416,798, 4%
- Other, 12,790,313, 3%
- Email, 1,015,599, 2%

Type of Entity by Number of Incidents (as of 2/15/15)

- Healthcare Provider, 757, 67%
- Business Associate, 272, 24%
- Health Plan, 106, 9%
- Healthcare Clearing House, 4, 0%
Reported Breaches Involving 500 or More Individuals
Type of Entity by Number of Individuals (as of 2/15/15)

- Healthcare Provider, 13,275,917, 32%
- Health Plan, 5,371,526, 13%
- Healthcare Clearing House, 17,754, 0%

Source: www.hhs.gov/ocr

Settlement Trends

- Lack of thorough and accurate risk analysis is leading issue
- Most recent settlements have come from reported breaches
- Multi-year delay between reporting of breach and settlement
- Office for Civil Rights looks for decisive action
- Substantial majority of breach investigations are closed without settlement or fine
Case Studies

Hypothetical (Employee Snooping)

- Employee snoops on record of patient (another employee) out of curiosity
  - PHI is fully identifiable and sensitive
  - Employee has violated policy, but no evidence of malice towards patient
  - PHI was definitely acquired
  - Employee has been sanctioned and agreed to not further use or disclose

- Has the information been “compromised”? 
Hypothetical (Stolen Laptop)

- Laptop is stolen from doctor’s office with password protection but no encryption. No SSNs are on the laptop.
  - PHI is fully identifiable and sometimes sensitive
  - In the hands of criminals, but no evidence that they have interest in the information
  - Cannot demonstrate that PHI has not been accessed
  - Risk has been slightly mitigated (password protected)

- Has the information been “compromised”?

---

Healthcare Business Process Outsourcer

**Situation**

- Building break in
- Numerous laptops stolen
- Two laptops used for analytics using thousands of patient records
- Organization is a HIPAA business associate to hundreds of clients, several of which were affected by the data analytics
Healthcare Business Process Outsourcer

Assessment

– Forensics was very time consuming because it was necessary to look at contents/attachments of thousands of emails
– Laptops were incorrectly configured to store messages/attachments locally
– Dataset included name, address, SSN, CPT codes, diagnosis codes. Incident risk assessment clearly concluded this was a breach

Healthcare Business Process Outsourcer

- Challenges and Lessons
  – Difficult to notify affected covered entities without unreasonable delay in cases such as this because of nature of forensics
  – Largest/most demanding clients prioritized highest and tend to be served better
  – Latent risks exist due to decision to not complete forensics nor notify other clients (covered entities) that may have been affected
Online Employee Benefits Portal

Situation

- Large client of this vendor was testing enterprise threat management software; turned up this vendors’ data on black market
- Vendor Initiated internal investigation, but limited usefulness due to system switchover within last several months
- Retained outside forensic investigator, confirmed old system had been compromised
- System served over 100 customers with 100s of thousands of employee health records
- Dataset included first name, last name, and email address

Online Employee Benefits Portal

Assessment

- While dataset typically wouldn’t be considered a “breach”, due to linkage with named client, it engendered much greater risk of successful phishing attack
- RADAR risk assessment resulted in “yellow” heatmap result (“possible breach”)
- Because of this, organization consulted several attorneys; got conflicting advice/opinions as to whether this incident constituted a “breach”
- They notified all clients (covered entities) of the incident and of their intention to do voluntary notification out of an “abundance of caution” if the client felt this was needed after their own review of the facts
Online Employee Benefits Portal

Challenges and Lessons

– Even with good forensics data, the breach/no breach decision is sometimes not black or white, and counsel often see gray areas

– This makes the decision of whether an incident is a breach, and/or to notify, one that is not just a legal but also a business decision

– In such circumstances, however, once notified of the BA’s intention, the clients (covered entities) will often request/require different/additional capabilities in the notification or the protection offering

For more information

Adam H. Greene, JD, MPH
adamsungreene@dwt.com
202.973.4213

Doug Pollack
doug.pollack@idexpertscorp.com
971.242.4724