The Adventures of Breach Reporting

Lessons Learned from Across the Country

Tools to Use to Identify Risk Areas and Close Gaps

Vendor Incident Management: What to Expect; What to Demand

Erika Bol, Privacy Officer, Colorado Department of Health Care Policy & Finance
Caron Cullen, SVP & Compliance Officer, Affinity Health Plan

It's not Just about HIPAA

- Know Your State Breach Reporting Laws
  - New York State: has a similar but different law around "natural persons" and what constitutes a reportable breach with 7 different places to report
  - Colorado: breach notification law deals with personally identifiable information (PII) held in electronic form
- Other Federal breach reporting requirements
  - FISMA, Information Security Act, GLBA, FTC, FCRA, OMB Memorandum M-07-16, etc.
- This presentation will focus on HIPAA/HITECH reporting

Office of Civil Rights

- **Region VIII - Denver (Colorado, Montana, North Dakota, South Dakota, Utah, Wyoming)**
- **Region II - New York (New Jersey, New York, Puerto Rico, Virgin Islands)**

How to Deal with HHS-OCR – and Why? (New York experience)

- Document everything… phone conversations with them… they will ask you about something you said in a prior conversation.
- Ask for extensions, when needed.
- Get Legal involved, if needed.
- Give them what they ask for:
  - Make sure you understand what OCR needs; why, if possible. It may help you deliver what they really want.
  - Push back when appropriate because…

Boxes of ePHI!

How to Deal with HHS-OCR (Colorado experience)

- Call them back when they call you
- Make sure you're answering the questions they are asking
  - Remember their Office's focus (civil rights!)
- Document what you tell them
- Learn from the experience so you don't repeat it next time

The Basics of Breach Reporting (Omnibus Final Rule)

- Are you dealing with PHI -- as defined in HIPAA?

Is there a Violation of the Privacy Rule?

- Does an exceptio n apply?

  3 statutory exceptions listed in IFR stay the same in Final Rule

Case #1: PHI or not?

Client DOB	Gender	ACRG3 Description	Condition Description	Total Allowed
06/17/1982	F	Multiple Minor	Asthma	5184.56
01/09/1973	M	Pairs – Multiple Dominant	Mental Health	40,565.45
08/16/1989	F	Multiple Minor Chronic	SA and Alcoholism	6675.11
10/19/1978	F	Catastrophic	Congestive Heart Failure	3511.78
3/22/2006	M	Health	Other	159.77
12/4/1993	F	Healthy Non-User	Other	0.00
04/12/1911	M	Single Minor Chronic	Other	1176.33

This was used by a provider to testify in front of Congress; then submitted as an attachment to that testimony. The provider lived in a small rural area.

Was the PHI *Unsecured*?

- Only ***unsecured*** PHI needs to be analyzed for potential breach reporting!

- *Not unsecured* if:
  - ePHI is encrypted (in accordance with current federal standards)
  - Paper PHI is shredded so that it can no longer be put reconstructed

NEW RISK ASSESSMENT!

- We must now ***presume*** that an acquisition, access, use, or disclosure of PHI (in a manner not otherwise permitted) ***is a reportable breach unless…***
- CE or BA ***demonstrates*** that there is a ***low probability*** that the PHI has been ***compromised***

Note: HHS expects us to change our policies & procedures before 9/23/2013 to reflect this!

Notification *not* required if demonstration, through Risk Assessment, that:

FINAL RULE

- there is a *low probability* that *PHI has been compromised*
  - Demonstrated through risk assessment
  - Four objective factors provided by HHS

INTERIM FINAL RULE

- there is no significant risk of harm to individual
  - Financial, reputation or other harm

4 Factors

TYPE?	WHO OR TO WHOM?	HOW OR HOW MUCH?	MITIGATION!
• The nature and extent of the PHI involved • Consider types of identifiers and likelihood of re-identification	• The unauthorized person who used the PHI or to whom the disclosure was made	• Whether the PHI was actually acquired or viewed	• The extent to which the risk to the PHI has been ***mitigated***

BREACH RISK ASSESSMENT

- Use a Tool!
  - Helps with Consistency
    - Provides common metrics for each incident
  - Helps with Documentation
    - Start it each time an incident is reported; add on as you go through process
  - Customize yours!
    - Include all of your State and Federal reporting requirements
  - OMB Memorandum M07-16
    - Lists factors to consider in assessing risk (of harm)
  - NCHICA Tool
    - Quantitative Scoring System
    - Sorts by variables such as Recipients, Circumstances of release, Disposition of information
  - Note: WE NEED UPDATED TOOLS for Final Rule

BREACH RISK ASSESSMENT

- Required if you are going to demonstrate low probability that PHI has been compromised and *not* notify

- Not required if you are considering the event a reportable breach under HIPAA and proceeding with notifications…

The Basics of Breach Reporting

- If you can't demonstrate a ***low probability that PHI has been compromised*** you must report to:
  - Affected individuals
  - Office of Civil Rights
  - The media (if applicable)
- Document, document, document.
- Not just a paper trail but every phone call; every contact to demonstrate what you have done to mitigate risks.

500 or more Affected Individuals

1. Notify individuals
2. Notify HHS concurrent with individuals (immediately)
3. Notify media
   - If 500 or more individuals in one State or jurisdiction

Currently 537 reported 'large' breaches since 9/2009

What about under 500 members?

- When do you report, if at all?
- What should be included in the report?
- Is there a standard?
- Do you use the same definition/assessment as with the large reports?

- Annually by March 1st
- http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html
- Yes, online.
- Get these done early in case you want Legal-blessing.

Speaking of which….

March 2013

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
					1	
3	4	5	6	7	8	
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Report to OCR

Enforcement of "small" breaches

- January 25, 2013
- HHS Settles with Hospice of North Idaho
  - $50,000
  - 441 individuals affected
  - Theft of unencrypted laptop
- October 29, 2012
- OCR inquiry into Colorado Medicaid reported breach of 124 individuals
  - BA sent out health insurance cards to incorrect individuals

Lesson: Size does not matter to OCR!

Know the Regulations; understand your interpretation of them

- Reportable breach per HIPAA
- Violation of an entity's policies &/or procedures

versus

- *Losing an unencrypted laptop or thumb drive*
- *Returning copier hard drives with ePHI (thank you CBS!)*
- *Sending an unsecured email with ePHI but the email was received by the intended recipient.*

Recognize Your or Your Privacy Officer's Personality

- Adjust your Harm Risk Assessment based on it!
- Be careful about what you report; be objective. Don't do it just because you feel bad or scared. Make sure it's what is required.
- Always a little gray. Use Legal Counsel when necessary.
- Risk tolerance. Personality traits – if you can't look at a situation and assess a situation, you're not doing your job.

The Spectrum of Risk Tolerance

50%

Wild, wild west cowboy (I've got this covered; no need to report it to the pesky gov't)

Where do you fall??

Mr. Rodgers (Let's report <u>everything</u> – *just* in case….)

Stuff Happens!

- No matter what you learn here today or what safeguards you put in place….
- Expect the Unexpected!

Complaint – RE: 3rd Party Vendor

- Whistleblower Complaint received and was sent to outside counsel for independence.
- The complaint had NOTHING to do with HIPAA/HITECH!
- As part of the investigation, attorneys looked through 20,000 emails, and
- Found that an employee sent her brother a spreadsheet and asked for Excel formatting assistance!
- It had for 933 members' names and other information on it.

Create an Interdisciplinary Team to deal with Incidents/Breaches

- Members:
  - HR
  - Legal
    Privacy
  - Information
    Technology/Security
  - Facilities
  - Compliance

Incident Response Plan

Some Actions:

- Create a charter
- Define who does what
- While you are busy with responding, don't forget to communicate to your employees.

Vendors

- Annual Assessment
  - After assessment is completed, define what is required vs. recommended, e.g.,
    - Data Leak Protection is required.
    - Hiring a Security Analyst is recommended.
- Annual Reporting to you of their "incidents/potential breaches." How does that happen?
  - Don't let your business associates tell you if it's a breach or not.
  - Let them pay the costs.
- You are the customer!

Case Example #2: Report or Not?

- Letter is mailed to 903 Members to tell them about a change in a vendor and the mailing address is:

  John Doe
  053149861A
  535 E. 14th Street, Apt #5A
  Seattle, WA 98101

- Found out that the number between name and address is the Head of Household's SS#
- Is this a Reportable Breach for HIPAA/HITECH?

Case Example #3: Report or Not?

- A claim is processed for Dr. Ralph Jones, a psychiatrist, for member Ms. Smith. The diagnosis and treatment is related to a behavioral health condition.
- The Claims Examiner incorrectly selects Dr. Robert Jones, a podiatrist. Dr. Robert Jones receives the Explanation of Benefits with Ms. Smith's information on it. Ms. Smith is not his patient.
- Both doctors are covered entities under HIPAA/HITECH.
- Is this a Reportable Breach in HIPAA/HITECH?

Top 10 Things We Would Do Differently

1. Don't assume someone in your organization won't steal your PHI for personal gain.
2. *Train* your employees on your incident reporting policy.
3. Enforce your Sanctions Policy <u>equally</u> across all of your workforce. (Do you have one written?)
4. Assume your vendors/business associates don't 'have your back.'
5. Have audit protocols for vendors that include a HIPAA/HITECH Security Review.
6. Hire an IT Security Analyst to monitor activities for the enterprise and collaborate with the Privacy Officer.

Top 10 Things …

7. Add technology solutions to safeguard ePHI, e.g., Data Leak Protection (DLP) or Iron Key – just remember nothing is 100% foolproof.
8. From the <u>*first moment you realize a breach happened*</u>, document every phone call or meeting you or your staff had with anyone.
9. Review all vendors – to make sure they have an updated Business Associate Agreement (e.g., Copier Leasing Vendors) which shifts the responsibility to them vs. covered entity.
10. Use company equipment only – no personal laptops, printers, copiers, etc.

The End

- Caron Cullen
  Sr. VP & Compliance Officer
  Affinity Health Plan
  (718) 794-5731
  ccullen@affinityplan.org
- Erika Bol
  Privacy Officer
  Colorado Department of Health Care Policy & Financing
  (303) 866-2958
  Erika.bol@state.co.us