


HIPAA Breach Notification: Case Studies on What to Do and When to Report


HCCA Managed Care Compliance Conference February 7, 2011

**Caron R. Cullen, VP of Compliance & Regulatory
Affairs, Affinity Health Plan**

**Elizabeth Callahan-Morris, Attorney,
Hall Render**



Affinity's In The News



The collage features several news items:

- Affinity Health Plan and/or its vendors... 400,000 of records**: A report from the Office of Inspector General regarding a data breach.
- Congress of the United States... House of Representatives**: A report from the House of Representatives regarding a security issue.
- Photocopier Fallout: Congress, FTC "Concerned"**: A CBS News Investigates article about a security vulnerability in copiers.
- Personal Information on the Copy Machine**: A CBS News Investigates article about how copiers can store personal information.
- Peter Cochrane's Blog: The hidden security threat in your office printers**: A blog post discussing the security risks of office printers.

Background Information

- 11/2005 - Affinity leased 34 copiers.
- The lease agreements indicated to return the copiers in the same manner as delivered except normal usage.
- 4/2009 to 6/2009 – Affinity returned 22 of the 34 leased copiers. Affinity still had 12 copiers under our control.

3

Tracking the Copiers

- Calls... calls... and, more calls... to determine where the 22 copiers were.
- Dealt with:
 - two different leasing agents, and
 - sales division of a major manufacturer.
- Finally, we learned that some of the copiers were shipped overseas.
- There was uncertainty as to when the hard drives might be returned.

4



HIPAA/HITECH Breach Notification Rule

- OCR Interim Final Rule published 08-24-09, effective 09-23-09:
 - Covered Entities (CEs) are required to notify individuals and HHS of breaches of unsecured protected health information (PHI).
 - Business Associates (BAs) causing such breaches are required to notify CE of such breaches.
- Sanctions for failure to notify began 02-22-10.
- Final Rule scheduled to be issued March, 2011.

5



Required Breach Notifications

- Breach notification is required when there is:
 - acquisition, access, use, or disclosure not permitted by the HIPAA Privacy Rule, of
 - unsecured PHI,
 - when exception does not apply, that
 - compromises security or privacy of such information.

6



Step 1: Violation?

- Determine if acquisition, access, use or disclosure was in violation of HIPAA Privacy Rule.
 - If not in violation of HIPAA Privacy Rule, not subject to the breach notification rule.

7



Step 2: Unsecured PHI?

- Determine if PHI was "unsecured."
- Unsecured PHI is PHI not secured through use of technology or methodology that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals, per HHS guidance.
 - HHS guidance: encrypted or destroyed PHI per NIST standards is considered secured, and not subject to breach notification rule.

8



Step 3: Exception?

- Determine if exception applies:
 - Unintentional acquisition, access, or use of PHI by workforce member or other person under authority of CE or BA, if in good faith, within scope of authority, and PHI not further used or disclosed.
 - Inadvertent disclosure of PHI by person authorized to access PHI to another such person at same CE, BA, or OHCA, and PHI not further used or disclosed.
 - Disclosure of PHI to person not reasonably able to retain such information.

9



Step 4: Compromises the Security or Privacy?

- Determine if breach "compromises the security or privacy" of PHI.
 - Determine whether it "poses a significant risk of financial, reputational, or other harm to the individual," per risk assessment.
 - Note: If PHI contained no identifiers (none of the 16 direct identifiers per limited data set rule, plus no dates of birth or zips codes), then it automatically does not "compromise the security or privacy" of PHI.

10

Affinity's Next Steps

- What's the Plan?
- Who is potentially affected?
 - Understand regulations and capture data
- Review both State and Federal requirements to cover all elements.
 - HIPAA / HITECH
 - 344,579 (Members)... PLUS
 - New York General Business Law – 899-aa
 - 65,038 (Employee, Members, other Individuals)
 - Total of potentially impacted customers –
 - 409,617

11

The Plan... Call

- Regulators
 - Attorney General's Office
 - New York State Department of Health
 - New York City Department of Health & Mental Hygiene
 - CMS
- Insurance Carrier

12

The Plan... Notification

- Prepare Notices – English, Spanish, and Chinese.
- Obtain Toll-Free Numbers (6).
- Hire a Call Center to handle the call volume.
- Create telephone scripts.
- Train internal staff (who were also affected parties).

13

Notification...

- Train External Call Center Staff.
- Prepare Press Release.
- Update Affinity's Website.
- Assign a Project Manager.
- Create and deliver mailing lists to vendor.
- Mail notices.

14

Notification... Federal

- Notice to the Secretary of HHS of Unsecured Protected Health Information.
- Call CMS IT Help Desk – Request a Computer Security Incident Report.

15

Other Activities and Suggestions

- Request current leasing agent to sign a BAA.
- Validate that copiers have encryption or overwrite feature and is it activated.
- Remove hard drives when lease expires.
- Update P&P for destruction protocol to include copiers.
- Create Process Improvement team to assess other potential risk areas.

16

What Now?

- Met with the NYS Attorney General's Office.
- Contact with HHS Office of Civil Rights indicating that an investigation has been opened. Must respond to a written inquiry within 20 days.
- **Education, Education, Education!**

17

Risk Assessment factors

- Risk assessment should consider:
 - Who impermissibly used PHI or to whom was PHI impermissibly disclosed.
 - What immediate steps were taken to mitigate impermissible use or disclosure?
 - Whether PHI was returned before accessed for improper use.
 - Type and amount of PHI.
 - Sensitivity of information contained in PHI.

18



Breach Notification Rule Preamble on Risk Assessments

For example, if a CE improperly discloses PHI that merely included the name of an individual and the fact that he received services from a hospital, then this would constitute a violation of the Privacy Rule, but it may not constitute a significant risk of financial or reputational harm to the individual.

In contrast, if the information indicates the type of services that the individual received (such as oncology services), that the individual received services from a specialized facility (such as a substance abuse treatment program 8), or if the PHI includes information that increases the risk of identity theft (such as a social security number, account number, or mother's maiden name), then there is a higher likelihood that the impermissible use or disclosure compromised the security and privacy of the information.

19



Case Study: Lost Jump Drives

- Two cases of lost jump drives
- Two risk assessments
- One required breach notification
- One did not require breach notification
- What was the difference?

20

Other Case Studies

- OCR breach report summaries
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>
- Snooping
- Facebook postings and blogs
- Misdirected faxes and letters
- Office break-in's

21

Comments and Questions

Caron R. Cullen
VP, Compliance & Regulatory Affairs
ccullen@affinityplan.org
718-794-5731

Elizabeth Callahan-Morris
Attorney, Hall Render
ecallahan@hallrender.com
248-457-7854