Identifying, Investigating and Responding to Suspected Breaches

Heather Campbell

Nancy Ruzicka

Michael Jenkins

Breaches

- Applies to “unsecured PHI”
- PHI not secured by use of a “technology or methodology” issued in “guidance” (published in FR April 27, 2009)
- Describes how to render PHI in paper or electronic form “unusable, unreadable, or indecipherable”
- Do not have to do this—but provides safe harbor if you do

Scenario

You are the privacy officer of a large healthcare provider. An employee leaves a message on your compliance hotline, telling you there has been an error in the transcription area that resulted in transcribed operative reports from your hospital being visible on the internet.

Identification and Investigation

- You have identified an issue that must be investigated
- Process of investigation
  - Who will conduct the investigation?
  - May be a person charged with investigating (Privacy Officer generally), but Privacy Officer is likely to need a fair amount of assistance in gathering relevant information (IT, transcriptionists, employee who reported the issue, etc.)
  - Per corporate policy, others must cooperate (and do so in timely manner) in the investigation

Investigation

- Oversimplified, but truly is:
  - Who
  - What
  - When
  - Where
  - Why
  - How

Investigation

- Who
  - Whose information was potentially compromised?
  - Who was involved/who do you need to talk with?
    - Employee who made the report
    - Transcriptionists
    - IT Security
    - Others

Employee Reporting and Discipline

- Employees who use or disclose PHI in violation of the Privacy or Security Rule, or who learn of a violation of the Privacy or Security Rule, must notify the Privacy Officer or designated individual.
- Cannot retaliate against employees who report HIPAA violations. Retaliation is against the law.

Investigation

- What-what information was potentially compromised?
  - Protected Health Information?
  - Encrypted?
  - Name, medical record number, diagnosis, procedure, etc.?

Investigation

- When
  - When did the incident occur?
  - Here the date that you were notified is important, but the date the employee who called you learned of it is perhaps more important
  - What period of time is covered- meaning how far back do the reports go, and how long have they been sitting unsecured on the internet
  - When did you last update your risk analysis?

Investigation

- Where
  - Where was the information generated/stored?
  - Where was it transmitted (if at all)?
  - Where was it “found” on the internet?
  - Where do the patients whose information was compromised live?

Investigation

- Why and how?
  - Why did this occur?
  - Human, system error?
  - Updates to system can sometimes cause vulnerabilities
  - Malicious software?
  - Other?

Investigation

- In the course of your investigation, you learned that a patient called the employee, Jane Doe, to complain that she found her operative report by searching her name on Google
- You learned that your transcription is performed by an outside vendor, who uploads the completed reports to their secure server prior to sending them back to your hospital
- You learned that approximately 350 operative reports with dates ranging over a period of 6 months in a one-year period were stored in a folder that during a system upgrade became unprotected due to failure to re-secure a folder on the system with a password protection

Breaches

- Impermissible use or disclosure is presumed to be a breach unless CE (or BA) can demonstrate that there is a low probability that the PHI has been compromised
  - Compromised- is there a significant risk of financial, reputational or other harm?
  - Notification necessary unless ***low probability*** is demonstrated
- Risk assessment necessary and document conclusion

Breach Notification

- Notification to individual “without unreasonable delay,” but no more than 60 days from discovery
  - “Discovery” is first day the breach is known to the covered entity, or the day the covered entity “would have known” had it exercised due diligence
  - Deemed to have knowledge if a workforce member knows (other than the person committing the breach)

Breach Notification

- Notification must include:
  - Brief description of what happened
  - Description of PHI involved
  - Steps the person should take to protect themselves from potential harm
  - Brief description of covered entity's investigation, mitigation, and protection from further breaches
  - Contact information for additional questions and information
    - Must include a toll-free number, email address, website, or postal address

Breach Notification

- How to notify:
  - First class mail to last known address (email ok if person has agreed to electronic notice)
    - If deceased, and address of next of kin or personal representative available, notify that person
    - If there is “possible imminent misuse,” may provide by phone or other appropriate means, in addition to first class mail
  - Use substitute form of notice if insufficient or incorrect contact information
    - If fewer than 10 people, use alternate form of written notice, phone, or “other means”
    - If more than 10, must post on home page (for 90 days) or major print newspaper or broadcast media; must include toll-free number that remains active for at least 90 days

Breach Notification

- If a breach involves more than 500 people, must also notify "prominent media outlets" serving the state or jurisdiction
- Government must be notified of ALL breaches
  - If more than 500 people, notify at the same time that individuals are notified
  - Otherwise, must maintain a log or other documentation of breaches and give that to HHS by March 1

Breach Notification

- There are companies who provide breach notification services, credit monitoring and support, including call center functions as ongoing support
- Can be a very cost-effective solution that should be considered with a large breach
- Often is covered by insurance (if you have the right coverage!)

Takeaways

- Do not delay in investigation
- Consider reputational harm in handling of response- although breach is harmful, bungling the response is likely worse
- Be transparent with patients, business associates and with government agencies
- Make sure you clearly identify what steps are being taken to prevent it from happening again
- Choose business partners wisely and ensure you have good business associate agreements that provide indemnification