Lessons Learned from Recent Data Breaches:

Strategies to Prepare for and Respond to a Breach

HIPAA Summit

March 17, 2015

Rebecca C. Fayed
The Advisory Board Company
2445 M St., NW
Washington, DC 20037
fayedr@advisory.com

Direct: 202-266-6145

www.advisory.com

Rebecca Williams, RN, JD
Davis Wright Tremaine LLP
1201 Third Avenue, Suite 2200
Seattle, WA 98101
beckywilliams@dwt.com

Direct: 206.757.8171

24/7 Data Breach Hotline:
844.GoToDWT (844.468.6398)

dwt.com

2014: The Year of the Data Breach?

Continuing through 2015?

dwt.com

Anthem

- 2nd Largest health insurance company.
- Holding company with numerous affiliates and works with independent Blue Cross & Blue Shield plans.
- Sophisticated cyber attack beginning December 2014.
- Access using high level credentials.
- More than 80 million people affected.
- 10 years' worth of consumer information.

  - Names, D/O/B, SSNs, addresses, employment and income data.
  - Not "medical information."
  - PHI.

Anthem Response

- Information disseminated (press releases, website, hotline, town hall meetings, customer reps).
- Offering identity theft protection for 2 years.
  - Automatically enrolled in protection but individual needs to sign up for monitoring (giving information).
- Notification.
  - HIPAA and state law.
  - Notice to all State AGs.
  - Notice to state consumer agencies.
  - Talking to OCR re HIPAA notification.
- Additional confusion/complications based on Anthem's role as insurance issuer and as a third party administrator for self funded health plans.

Preparation for a Breach: A Vulnerable Sector

Data Breach Incidents by Sector, 2013

Source: Norton Cybercrime Index

Industry Sector	Number of Incidents	Percentage of Incidents
Healthcare	93	36.8%
Education	32	12.6%
Government and Public Sector	22	8.7%
Retail	19	7.5%
Accounting	13	5.1%
Computer software	12	4.7%
Hospitality	10	4.0%
Insurance	9	3.6%
Financial	9	3.6%
Transportation	6	2.4%
Information technology	5	2.0%
Telecom	4	1.6%
Law enforcement	4	1.6%
Social networking	3	1.2%
Agriculture	2	0.8%
Community and non-profit	2	0.8%
Administration and human resources	2	0.8%
Military	2	0.8%
Construction	1	0.4%
Utilities and energy	1	0.4%
Computer hardware	1	0.4%

Internet Security Threat Report 2014: Volume 19, Appendix A; Symantec Corporation

10-Step Breach Response Plan Overview

1. Prepare for the possibility/eventuality of a breach.
2. Investigate.
3. Stop the harm, mitigate, and take corrective action.
4. Assess and document whether the event is a “breach” under HIPAA.
5. Analyze whether event is a breach under applicable state law.
6. Notify individuals (or the covered entity).
7. Notify HHS.
8. Notify the media and others (maybe).
9. Reassess: What can be learned from the event?
10. Wrap up and prepare for possibility of investigation/audit.

Step 1:
Prepare for the Possibility of a Breach

- Develop, implement, and document an incident response and breach notification process.
  - Test the incident response process.
- Develop/revisit Security Rule risk analysis.
- Establish an incident response team.
  - Internal Team including the point of contact.
  - External Team (attorneys, forensic experts, breach response firms, etc.)
- Consider encrypting PHI.
- Train workforce!
  - What to report.
  - Who to go to with concerns and questions.

Step 1:
Prepare for the Possibility of a Breach

- Business Associates and Subcontractors
  - ➢Due diligence on business associates.
  - ➢Know your business associates, and subcontractor/business associates; know what they do.
  - ➢Maintain a list with contact information.
  - ➢Document management system.
  - ➢When negotiating business associate contracts, consider:
    - Indemnification.
    - Addressing responsibilities in the event of breach notification.
    - Timing for reporting breach, impermissible use or disclosure, and security incident.
    - Mitigation.

Step 1:
Prepare for the Possibility of a Breach

- Consider cyber insurance
- Review any existing policies to verify:
  - Coverage.
  - Whether you can use the outside support you choose.

Step 2:
Investigate the Event

- Activate incident response and breach notification process.
  - If no process, identify individuals in the best positions to help investigate and respond to the incident.
- Identify:
  - Facts surrounding the incident: who, what, where, when, how, and why (e.g., stolen or lost laptop, backup tape, portable storage device; email or fax sent to wrong recipient; paper records thrown in the trash).
  - Type of information involved: PHI? PII? (e.g., names, addresses, PHI, SSNs, credit card numbers).
  - Number of people affected.
  - States in which affected people live and total in each state.
  - Whether the information was encrypted.
  - Whether information systems were affected.

Step 3:
Stop the Harm, Mitigate, & Take Corrective Action

- Stop the Incident!
- Preserve and secure evidence, including log files.
- Decide whether to contact law enforcement (e.g., police, FBI).
- Recovery - return systems to normal.
- Mitigate - A covered entity or business associate must mitigate, to the extent practicable, any harmful effect that is known to the entity of an impermissible use or disclosure of PHI.
  - For example, contact recipient and ask for information to be returned or destroyed.

Step 3:
Stop the Harm, Mitigate, & Take Corrective Action

- Corrective action - may need to
  - Terminate agreement with business associate.
  - Revise procedures.
  - Sanction employees.
  - Do additional training.
- Decide whether to offer:
  - Credit monitoring services.
  - Identity theft services.
  - Other support for affected individuals.

Step 4:
Assess and Document Whether Incident is a Breach under HIPAA

- Breach:
  - Acquisition, access, **use**, or **disclosure**
  - Of **PHI** (either electronic or hard copy)
  - **Not permitted by the Privacy Rule** that
  - **Compromises** the security or privacy of PHI

Step 4:
Assess and Document Whether Incident is a Breach under HIPAA

- Steps to Determine if Incident is a Breach:
  - Impermissible use or disclosure of PHI under Privacy Rule?
  - Compromises the privacy or security of PHI?
  - Excluded from the definition of a breach?
    - An unintentional use of PHI by a workforce member acting in good faith and within the scope of his or her authority, and the PHI is not further used or disclosed improperly;
    - An inadvertent disclosure of PHI by an authorized person to another authorized person, and the PHI is not further used or disclosed improperly; or
    - A disclosure of PHI to an unauthorized person where there is a good faith belief that the unauthorized person would not reasonably have been able to retain the PHI.

Step 4:
Assess and Document Whether Incident is a Breach under HIPAA

- Presumption of breach
  - Unless a *low probability of compromise* is demonstrated based on a
    - documented breach risk assessment
- Risk assessment of at least:
  - Nature of PHI (e.g., identifiability, sensitivity).
  - Unauthorized recipient (e.g., subject to confidentiality requirements).
  - Whether PHI was actually acquired or viewed.
  - The extent that risk has been mitigated.

Step 4:
Assess and Document Whether Incident is a Breach under HIPAA

- HIPAA breach notification requirement applies only to the breach of unsecured PHI.
- The breach of secure PHI is not subject to the breach notification.
- If PHI is rendered "unusable, unreadable, or indecipherable" to unauthorized individuals, it is secure.
- Technologies and methodologies that will render PHI secure:
  - Encryption.
  - Destruction.
- Safest course: Encrypt! Encrypt! Encrypt!

Step 5:
Analyze Whether Incident is a Breach under State Law

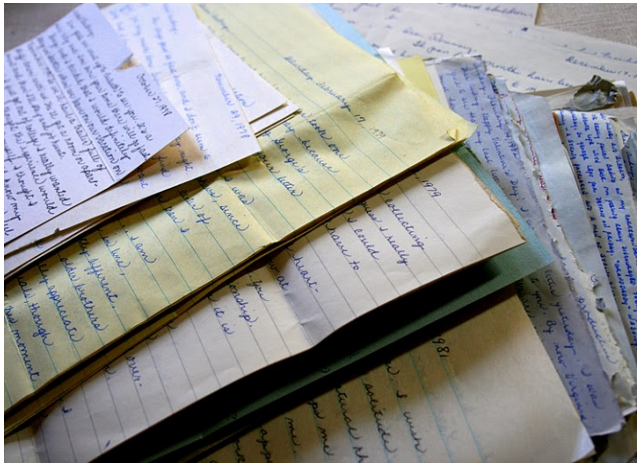
- Vast majority of states have data breach notification laws.
- Verify state law's definition of "personal information."
- Determine any exceptions to breach notification obligations (e.g., encryption, harm-based standards).
- If state breach notification law is triggered, state notification obligations may exist in addition to HIPAA.
- Most state laws allow a single notification to address both state and HIPAA requirements (beware of Massachusetts).

Step 6:
Notify Individuals

- HIPAA: Covered entity must provide notice to the individual "without **unreasonable delay**" and no later than 60 days after breach is discovered.
  - Notification should be made sooner than 60 days if possible.
  - But avoid premature notification.
  - Subject to law enforcement delay.
- Pay attention to state timing requirements.
- Discovery: When any workforce member or agent knew or should have known of the breach (excluding person committing the breach).

Step 6:
Notify Individuals

- Covered entities must notify affected individuals:
  - Via first-class mail.
  - Unless the individual has consented to email.
  - Substitute notice may be required if not able to contact people.
- Notice must include:
  - Description of facts about breach.
  - Type of PHI involved.
  - Steps individuals should take to protect themselves.
  - What the covered entity is doing to investigate the situation and prevent future breaches.
  - Contact information.



Step 6:
Or Notify the Covered Entity

- HIPAA business associates must notify covered entity of the breach **without unreasonable delay** and no later than 60 days after discovery.
- Notice to include, to the extent known:
  - Identity of affected individuals.
  - Information that covered entity must include in its notice.
- Business associate contract may address:
  - Who will make the notifications.
  - Who will pay for notifications.
  - Shorter notification time period.
  - Additional requirements for notification of breach, impermissible use or disclosure, or security incident.
- Goal: Individuals should not receive duplicative notices for the same breach.

Step 7:
Notify HHS

- Covered entities must notify HHS of the breach:
  - If more than 500 affected individuals – must notify HHS contemporaneously with notification to the individual via online notification.
  - If fewer than 500 affected individuals – must maintain a log and notify HHS no later than 60 days following the end of the calendar year in which the breach was discovered.
    - On-line notification
    - Promises the ability to enter log but for now each breach needs its own notification.

Step 8:
Notify Media and Others

- Possible Media Notification
  - ➢ If PHI of more than 500 individuals in one state is breached, covered entity must notify “prominent media outlets” in the state.
  - ➢ Different from substitute notice.
  - Check state laws to determine whether any additional notifications must be made (e.g., consumer protection agencies, Attorney General’s office, consumer reporting agencies).

Step 9:
Reassess: What Can be Learned from the Event?

- Compliance policies and procedures:
  - ➢Evaluate and revise if they do not work for the organization or do not adequately safeguard PHI.
    - For example:
    - ✓If incident involved lost or stolen backup data tape, consider changing procedure for transport and/or storage.
    - ✓If incident involved faxing information to a wrong number, consider changing procedure to require contacting the intended recipient before the fax is sent to confirm number and after the fax is sent to confirm receipt.
- Risk analysis:
  - ➢ Revisit and update, if appropriate.

Step 9:
Reassess: What Can be Learned from the Event?

- Training: Security incidents presents learning opportunities.
  - If incident was the result of employee error, consider focused retraining of particular employees and general reinforcement.
- If incident was the result of a business associate's error:
  - Verify business associate's mitigation and corrective action.
  - Consider terminating the agreement or imposing more stringent safeguards under the agreement.
- Sanction workforce, as appropriate.

Step 10
Wrap Up and Prepare for Possible Investigation or Audit

- HHS-OCR investigated every “large” breach.
- Each OCR region receives report about “smaller” breaches in its region.
- OCR trained state AGs on HIPAA enforcement.
- Investigations have been initiated via letter and by phone.
- **OCR expects cooperation**.
- Generally, OCR has been asking for:
  - Facts surrounding the breach.
  - Copies of notification letters, media notices, business associate agreements.
  - Actions taken to locate missing data, prevent further loss of data, and protect affected individuals.
  - Security Rule risk analysis.
  - Description of safeguards in place to protect the information, specifically including whether data was encrypted.
  - Compliance efforts related to policies and procedure revisions, training, and sanctions imposed.

Step 10
Wrap Up and Prepare for Possible Investigation or Audit

- Finalize documentation of incident – while it is at front of mind.
  - Breach – whether incident was a breach, including risk assessment.
  - Notification – timely and appropriate (e.g., individual, HHS, media, substitute, other required agencies).
  - Security incident report (under Security Rule).
  - Reporting under business associates contract (impermissible uses and disclosures, security incident, breach).
- Track for accounting of disclosure.
- Checklist may be helpful.

- Remember: Covered entity and business associates have burden of proof that notification was appropriate.

QUESTIONS?

Rebecca C. Fayed
The Advisory Board Company
2445 M St., NW
Washington, DC 20037
202-266-6145
fayedr@advisory.com

Becky Williams
Davis Wright Tremaine LLP
1201 Third Avenue, Suite 2200
Seattle, WA 98101
206.757.8171
beckywilliams@dwt.com

DISCLAIMER

These materials should not be considered as, or as a substitute for, legal advice and they are not intended to nor do they create an attorney-client relationship. Because the materials included here are general, they may not apply to your individual legal or factual circumstances. You should not take (or refrain from taking) any action based on the information you obtain from these materials without first obtaining professional counsel. The views expressed do not necessarily reflect those of the firm, its lawyers, or clients.