PRESENTATION

Cyber Risks: Data Dos and Don'ts

HCCA Atlanta Regional Conference
January 20, 2017

Gina Ginn Greenwood, JD, CIPP/US
Monarch Plaza, Suite 1600
3414 Peachtree Road, N.E.
Atlanta, GA 30326
Office: 404.589.0009 ext. 1804
Cell: 404.909.0665
ggreenwood@bakerdonelson.com

BAKER DONELSON EXPAND YOUR EXPECTATIONS®

Overview

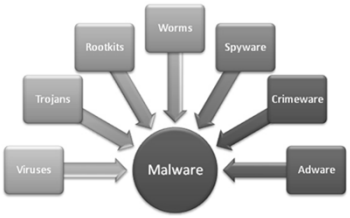
- How to Prepare For and Prevent a Data Breach
  - Latest Threats
- Enforcement
  - Evolution
  - New Twists

Cyber Risks in 2017

- Me, Myself and I -- WE are still our biggest risk: Employee Error
  - Unencrypted Laptops and Flash Drives – Still #1!!
  - Failure to Shred
  - Failure to Clean Drives Before Discarding
  - Clicking on the Wrong Link
    - Malware – Ransomware - evolved beyond crazy!
- Business Associates
  - Lack of Compliance, Understand or Care
    - Not willing to spend the $ to avoid the risk
  - Overseas Access – "If you want 24/7 technician help, we need to allow our overseas technicians to access."
  - Failure to Perform Due Diligence

How many types of Malware were LAUNCHED last year?

300,000,000



2017 New Year's Resolutions

- **DO** -
  - Gap Analysis
  - Risk Assessment
  - Risk Management Plan
  - Policies & Procedures
  - Consent Forms
  - Due Diligence – BAs
  - Auditing / Tabletops Exercises
  - Proper NOPP
  - Workforce Alerts
  - Document Incidents
  - BAAs in place
- **DON'T** –
  - Give in to unreasonable BAs
    - indemnification
    - limitation of liability
    - unreasonable access
    - unreasonable uses
    - due diligence
  - Assume anything !!
  - Give up hope !!

HIPAA / HITECH Breach Notification Rule Definition of "Breach"

"Breach" shall mean the acquisition, access, use, or disclosure of Unsecured Protected Health Information ("PHI") in a manner not permitted under HIPAA Privacy Rule which compromises the security or privacy of the PHI.

***Exceptions to Definition of Breach* -**
"Breach" shall exclude the following:

i. Any unintentional acquisition, access, or use of Unsecured PHI by a workforce member or person acting under the authority of a Covered Entity or a Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule.

Definition of "Breach" (Exceptions) (continued)

ii. Any inadvertent disclosure by a person who is authorized to access Unsecured PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the same Covered Entity or Business Associate, or organized health care arrangement in which the Covered Entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule.

iii. A disclosure of Unsecured PHI where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Definition of "Breach" (continued)

Except as provided above an acquisition, access, use, or disclosure of Unsecured PHI in a manner not permitted under the HIPAA Privacy Rule is presumed to be a Breach unless the Covered Entity demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
ii. The unauthorized person who used the PHI or to whom the disclosure was made;
iii. Whether the PHI was actually acquired or viewed; and
iv. The extent to which the risk to the PHI has been mitigated.

Assess the 10 Steps You Take When You Have a Data Breach

Best Defense is a STRONG Offense

Step One: Investigate and Mitigate Potential Breach

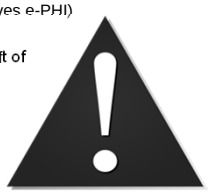
The investigation should include the following (as applicable):

- Interviews of knowledgeable persons, workforce members and/or Business Associate;
- Interviews of potential privacy/security violators;
- Forensic examination of computer hardware, software, etc. to determine extent of potential Breach and to determine what exact information was Breached, if applicable
- Communication with police officers to file theft or other reports and to review the police report(s).
- Etc.

Step Two: Alert Appropriate Parties

Covered Entity should alert KEY persons as soon as possible if a Breach is believed to have occurred:

- CEO/Administrator
- HIPAA Security Officer (if the Breach involves e-PHI)
- Local Police (if the Breach involves the theft of information)
- Liability Insurance Carrier
- Chairman of the Board of Directors, etc.



Step Three: Documentation Regarding -- Is a HIPAA / HITECH Breach Notification Required?

Once the investigation has concluded, the Covered Entity should ask the following questions to make a determination of whether a Breach of Unsecured PHI has occurred that requires notification:

A. Was there an acquisition, access, use, or disclosure of PHI?

B. Was the PHI at issue "Unsecured PHI"?

Step Three: Is a HIPAA Breach Notification Required? (continued)

C. Did the acquisition, access, use, or disclosure of PHI result in a violation of the HIPAA Privacy Rule?

D. Has the Covered Entity demonstrated (on paper) that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

ii. The unauthorized person who used PHI or to whom the disclosure was made;

iii. Whether the PHI was actually acquired or viewed; and

iv. The extent to which the risk to the PHI has been mitigated?

Step Three: Is a HIPAA Breach Notification Required? (continued)

E. Does an exception to the definition of Breach apply? *(See exceptions in definition of Breach at the beginning of this Presentation.)*

Step Four: Notice may not be is required by HITECH But May Be Required by State Law, etc. or State Law May Add Elements

Although there may not have been a Breach **requiring** HIPAA / HITECH notification, determine whether notice is advisable under the circumstances or is required under other federal, state or other laws that may be applicable.

- STATE LAW -- NIGHTMARE TO KEEP UP WITH!!
- Read state laws carefully -
  - Definition of Personal Info
  - Substitute notice
  - Content requirements
  - AG notice
  - Identity theft protection

Step Five: Notification of the Individual Whose PHI Has Been Breached Under HIPAA / HITECH

- The Covered Entity should following the discovery of a Breach of Unsecured PHI, notify in writing each individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such Breach.
  - Notice must contain all the required elements. See regulations!
  - Notice must be sent without unreasonable delay – no later than 60 days of discovery (or when Covered Entity should have known).
    - Standard: 2-4 days now!!
  - Substitute public media notice may be required.

Also determine whether any other federal or State laws apply that may require notification or other actions or special notice language.

Step Six: Notification of Media of Breaches involving 500+

For a Breach of Unsecured PHI involving more than 500 residents of a state or jurisdiction, Covered Entity shall, following the discovery of the Breach notify prominent media outlets serving the State or jurisdiction.

- *Timeliness of notification.* Media notification should be made **without unreasonable delay** and in no case later than 60 calendar days after discovery of a Breach.
- *Content of notification.* The media notification required shall meet the same contents requirements of the individual notice.
  - (NOTE: This notification typically should be made in the form of a press release and is a separate notification from the notification required under substitute notice provisions. The press release must be submitted to media but need not be printed.)

Step Seven: Notification of HHS

The Covered Entity shall, following the discovery of a Breach of Unsecured PHI, notify the Secretary of HHS using the electronic forms located on the HHS OCR Website at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

- ***Breaches Involving 500 or More Individuals.*** For Breaches of Unsecured PHI involving 500 or more individuals, the Covered Entity shall provide the notification required **contemporaneously with the individual notice** and in the manner specified on the HHS OCR Website.
- ***Breaches Involving Less Than 500 Individuals.*** For Breaches of Unsecured PHI involving less than 500 individuals, the Covered Entity **shall maintain a log** or other documentation of such Breaches and, **not later than 60 days after the end of each calendar year, shall provide notification** for Breaches discovered during the preceding calendar year, in the manner specified on the HHS OCR Website.

Step Eight: Accounting of Disclosures

Covered Entity should account for disclosures of PHI as required by the HIPAA Privacy Rule – 45 C.F.R. § 164.528.

Step Nine: Sanctions

Covered Entity should determine whether sanctions of a workforce member or Business Associate are warranted and should ensure such sanctions are administered in accordance with Workforce Sanctions Policy and/or Business Associate Agreements (if applicable).

- **Remember -- Need Cooperation**

Step Ten: Plan of Correction

Breaches should be assessed to determine the cause of the Breach and a corrective action plan should be developed by the HIPAA Privacy/Security Officer to try to prevent such Breaches in the future. Breaches of e-PHI should be assessed as part of the HIPAA Security Rule risk analysis/assessment. Documentation of the all corrective actions should be maintained. Correct within 30 days!!

- Review and Revise Policies and Procedures
- Re-train
- Monitoring

Gina Ginn Greenwood, JD, CIPP/US

Monarch Plaza
3414 Peachtree Road, N.E.
Suite 1600
Atlanta, Georgia 30326

Direct: 404.589.0009 ext. 1804
Cell: 404.909.0665
ggreenwood@bakerdonelson.com

BAKER DONELSON

- Gina Greenwood is a healthcare attorney and IAPP Certified Information Privacy Professional (US) who assists clients across the country with data and other compliance needs, data breaches and internal and external compliance investigations.
- Gina concentrates her practice on a wide range of health care and privacy/security matters, including cyber liability, risk management, data breaches and response, HIPAA Privacy and Security Rule compliance and HIPAA / HITECH breaches; PCI, COPPA, CAN-SPAM, TCPA Act, FTC Act, GLBA, GINA, Part 2, etc. compliance, meaningful use audits, fraud and abuse compliance and investigations, corporate health care transactions and day to day compliance advice to hospitals and other licensed health care entities.
- Gina has authored numerous materials including privacy and security policy manuals, licensure policy manuals, and Internet-based employee training modules.
- Gina has been recognized by Chambers USA as a leading health care lawyer in America and has been voted *Georgia Trend Magazine* Legal Elite. She served as 2014 expert legal witness on EMTALA and mental health issues during the USCCR hearings in Washington, DC. – which provided testimony to US Congress and President of the United States.