HCCA 2017 ST. LOUIS REGIONAL AREA COMPLIANCE CONFERENCE RENAISSANCE ST. LOUIS AIRPORT HOTEL MARCH 3, 2017

Cyber Security, What's New?

Anthony J. Munns, CISA, FBCS, CITP
Partner, Advisory Services
amunns@bswllc.com
Brown Smith Wallace LLP
314.983.1297 Direct
314.614.6582 Cell

Agenda

- Fundamentals of the HIPAA Privacy and Security Rules
- Breaches in the News
- Ransomware is Growing Fast
- How do we Reduce Risk
- Question and Answer

Disclaimer: The views and opinions expressed in this presentation are those of the presenters and do not necessarily reflect the official policy or position of any agency of the U.S. government. Whilst all information in this document is believed to be correct at the time of writing, the information in this presentation is for educational and awareness purposes only. For legal advice, please consult an attorney.

2

Learning Objective #1

Fundamentals of the HIPAA Privacy and Security Rules

3

Overview of Fundamentals

- OCR Website- Summary of HIPAA Privacy Rule: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
- HIPAA Administrative Simplification Regulations: https://www.hhs.gov/hipaa/for-professionals/index.html
- OCR Case Examples and Resolution Agreements: http://hhs.gov/ocr/privacy/hipaa/enforcment/examples/index.html
- OCR Frequently Asked Questions: http://www.hhs.gov/privacy/hipaa/faq/index.html

OCR Launches Newly Redesigned Website – January 6, 2016

Over the past several months, OCR has undertaken a full redesign of our website. We are thrilled to share with you the new www.hhs.gov/ocr, a more responsive, user-friendly platform.

4

2016 Updates

- March 21, 2016 **. OCR Launches Phase 2 of HIPAA Audit Program**
  - July 2016 - 167 Covered Entities notified of selection to participate in HIPAA desk audits
  - April 2016 – OCR quietly announces a ne Audit Protocol (see next slide)
  - On site audits to begin early 2017 - Will evaluate auditees against comprehensive set of HIPAA compliance controls
- April 15, 2016 FTC releases new web-based Mobile Health Apps Interactive Tool to help health app developers find out which federal laws to follow
- May 13, 2016 HHS finalizes rule to improve health equity under the Affordable Care Act - Final rule prohibits discrimination based on race, color, national origin, sex, age or disability; enhances language assistance for individuals with limited English proficiency; and protects individuals with disabilities. In addition to implementing Section 1557's prohibition on sex discrimination, the final rule also enhances language assistance for people with limited English proficiency and helps to ensure effective communication for individuals with disabilities.

New Audit Protocol

Federal regulators have quietly released an updated protocol for use in phase two of HIPAA compliance audits of covered entities and business associates this year. Here is the link: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol-current/index.html

The OCR HIPAA Audit program analyzes processes, controls, and policies of selected covered entities pursuant to the HITECH Act audit mandate. OCR established a comprehensive audit protocol that contains the requirements to be assessed through these performance audits. The entire audit protocol is organized around 3 modules, representing separate elements of **privacy, security,** and **breach notification**..

- The audit protocol covers Privacy Rule requirements for (1) notice of privacy practices for PHI, (2) rights to request privacy protection for PHI, (3) access of individuals to PHI, (4) administrative requirements, (5) uses and disclosures of PHI, (6) amendment of PHI, and (7) accounting of disclosures.
- The protocol covers Security Rule requirements for administrative, physical, and technical safeguards
- The protocol covers requirements for the Breach Notification Rule.

Note: the protocol has been updated to reflect the Omnibus Final Rule.

- July 19, 2016 HHS OCR Offers New Materials for Covered Entities - As of Monday, July 18, 2016, certain health care and coverage providers are subject to new requirements under Section 1557 and are expected to ensure their programs are in compliance with the law. HHS OCR has added a number of downloadable resources to our website to reduce burden for covered entities. Certain parts of the rule have a delayed applicability date and we encourage covered entities to review the procedural requirements<http://www.hhs.gov/sites/default/files/2016-06-07-section-1557-final-rule-summary-508.pdf> of the final rule.

  Materials include – training materials, Sample documents of a Notice of Nondiscrimination, Statement of Nondiscrimination and Taglines available for download in 64 languages, fact sheets on key provisions and frequently asked questions translated into the top 15 languages.

- July 27, 2016 OCR Announced that it had posted Guidance for the 2016 HIPAA Desk Audits and a New FAQ: HIPAA and Unique Device Identifiers. Identifiers (UDI), which clarifies that the device identifier (DI) portion of a UDI can be part of a limited or de-identified data set as defined under HIPAA. While the HIPAA Privacy Rule prohibits the inclusion of "device identifiers and serial numbers" in both limited data sets and data sets that are de-identified in accordance with the "de-identification safe harbor" provisions, the guidance explains that the DI portion of the UDI is not the type of "device identifier" to which these HIPAA Privacy Rule provisions refer.

- September 28, 2016 OCR Releases New FAQ on Availability of PHI Maintained by a Business Associate as to whether a BA of a HIPAA CE may block or terminate access by the CE to the PHI maintained by the BA for or on behalf of the CE (e.g.: an EHR developer seeking payment), clarifying that BAs may not use such information in a manner or to accomplish a purpose or a result that would violate the HIPAA Rules.

- October 7, 2016 OCR announced Cloud Computing Guidance.

- November 28, 2016 OCR issued an alert for a Phishing Email Disguised as an Official OCR Audit Communication! The phishing email is being circulated on mock HHS Departmental letterhead under the signature of OCR's Director, Jocelyn Samuels. If you look closely the email comes from the hhs-gov.us domain, not hhs.gov.
- December 20, 2016 OCR announced a new fact sheet on HIPAA and Public Health Permitted Uses and Disclosures.

9

Learning Objective #2

Breaches in the news

10

2016 Healthcare Data Breaches

- March 3, 2016 OCR Announces $1.55 million settlement with North Memorial Health Care of Minnesota - underscores the importance of executing HIPAA business associate agreements
- March 17, 2016 OCR Announces Improper disclosure of research participants' protected health information results in $3.9 million HIPAA settlement – Feinstein Institute for Medical Research (Manhasset, NY)
- April 20, 2016 OCR Announces $750,000 settlement with Raleigh Orthopaedic Clinic, P.A. for disposal of X-Rays highlights the need for HIPAA business associate agreements
- April 21, 2016 –OCR announces Unauthorized Filming for "NY Med" Results in $2.2 Million Settlement with New York Presbyterian Hospital

11

- July 18, 2016 OCR Announces Widespread HIPAA Vulnerabilities result in $2.7 million settlement with Oregon Health & Science University. During the investigation, OCR determined that UMMC was aware of risks and vulnerabilities to its systems as far back as April 2005, yet no significant risk management activity occurred until after the breach
- July 27, 2016 OCR Announces Multiple alleged HIPAA violations dating back to 2005 result in $2.75 million settlement with the University of Mississippi Medical Center
- August 4, 2016 OCR Announces Advocate Health Care of Illinois Settles Potential HIPAA Penalties for **$5.55 Million. This significant settlement, the largest to-date against a single entity**, is a result of the extent and duration of the alleged noncompliance (dating back to the inception of the Security Rule in some instances), the involvement of the State Attorney General in a corresponding investigation, and approximately 4 million individuals whose information was affected by Advocate.

12

- September 23, 2016 OCR Announce HIPAA settlement with Care New England Health System (CNE) of $400,000 with a CAP for the loss of unencrypted backup tapes containing the ultrasound studies of approximately 14,000 individuals. It illustrates the importance of reviewing and updating, as necessary, business associate agreements

- October 18, 2016 OCR Announced that $2.14 million HIPAA settlement with St. Joseph Health (SJH) underscores importance of managing security risk. A server SJH purchased to store files included a file sharing application whose default settings allowed anyone with an internet connection to access them.

- November 22, 2016 UMass settles potential HIPAA violations following malware infection with a CAP and monetary payment of $650,000 (reflective of the fact that the University operated at a financial loss in 2015). UMass had failed to designate all of its health care components when hybridizing, incorrectly determining that while its University Health Services was a covered health care component, other components, including the Center where the breach of ePHI occurred, were not covered components.

- January 10, 2017 OCR announced that Presence Health, one of the largest health care networks serving Illinois has agreed to settle potential violations of the HIPAA Breach Notification Rule by paying $475,000 and agreeing to implement a CAP. This is the **first HIPAA settlement based on the untimely reporting of a breach** of unsecured protected health information (PHI).

- February 1, 2017 OCR announced that they had initiated an investigation of Children's Medical Center Dallas based on several breach reports dating back to 2010. OCR determined that Children's Health violated the following provisions of HIPAA:
    - Access controls –encryption and decryption (45 CFR 164.312(a)(2)(iv))
    - Device and media control (45 CFR 164.310(d)(1))
    - Impermissible disclosures (45 CFR 164.502(a))

  On January 17, 2017 OCR confirmed that Children's had not filed an appeal and proceeded to issue a Notice of Final Determination (NFD) in the amount of $3.217 million. **First HIPAA case in which covered entity failed to file a timely request for a hearing**.

- February 16, 2017 OCR announced that Memorial Healthcare Systems (MHS) has paid the HHS $5.5 million to settle potential violations of HIPAA and agreed to implement a robust corrective action plan. MHS is a nonprofit corporation which operates six hospitals, an urgent care center, a nursing home, and a variety of ancillary health care facilities throughout the South Florida area. MHS is also affiliated with physician offices through an Organized Health Care Arrangement (OHCA).

  MHS reported to OCR that the PHI of 115,143 individuals had been impermissibly accessed by its employees and impermissibly disclosed to affiliated physician office staff. This information consisted of the affected individuals' names, dates of birth, and social security numbers. **The login credentials of a former employee of an affiliated physician's office had been used to access the ePHI maintained by MHS on a daily basis without detection from April 2011 to April 2012**, affecting 80,000 individuals. Although it had workforce access policies and procedures in place, MHS failed to implement procedures with respect to reviewing, modifying and/or terminating users' right of access, as required by the HIPAA Rules. Further, MHS failed to regularly review records of information system activity on applications that maintain ePHI by workforce users and users at affiliated physician practices, despite having identified this risk on **several risk analyses** conducted by MHS from 2007 to 2012.

15

Learning Objective #3

Ransomware is Growing Fast

16

So what is next…

Recently, one of the largest growth areas: Ransomware

- Hollywood Presbyterian Medical Center (HPMC): February 2016 Hackers took control of the hospital's computer systems. The hospital paid approximately $17,000 via 40 bitcoins to the hacker to get its files back. Note: Initial reports that the hacker wanted $3.6 million via 9,000 bitcoins were incorrect.
- Lukas Hospital, Neuss, Germany, suffered an infection in February, after the malware arrived attached to an email. The hospital had complete backups, and noted that all patient data was already encrypted. The hospital took all of its systems offline until they were fully restored, rescheduled 20 percent of its surgeries and shifted less-severe emergency care to neighboring hospitals.
- In January, Titus Regional Medical Center, Mount Pleasant, Texas, reported that ransomware had encrypted files on multiple database servers. "We couldn't get to our data," TRMC spokeswoman Shannon Norfleet told local newspaper The Daily Tribune. "When the computers went down and the network administrators accessed the network, there was the ransomware code."

17

Ransomware: Can't Hide from HIPAA

- A recent U.S. Government interagency report indicates that, on average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015).
- Ransomware is a type of malware (malicious software) distinct from other malware .
- Defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid.
- After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key.

18

Ransomware Can't Hide from HIPAA (Cont.)

- The HIPAA Security Rule requires implementation of security measures that can help prevent the introduction of malware, including ransomware. Some of these required security measures include:
- implementing a security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI) and implementing security measures to mitigate or remediate those identified risks;
- implementing procedures to guard against and detect malicious software;
- training users on malicious software protection so they can assist in detecting malicious software and know how to report such detections; and;
- implementing access controls to limit access to ePHI to only those persons or software programs requiring access.

19

Ransomware Can't Hide from HIPAA (Cont.)

Security Incident:

- A security incident under the HIPAA Rules is "…the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." See 45 C.F.R. 164.304.
- The presence of ransomware on a covered entity's or business associate's computer systems is a security incident.
- If a ransomware attack is detected the affected entity should immediately activate its security incident response plan, which should include measures to isolate the infected computer systems in order to halt propagation of the attack.

20

Ransomware Can't Hide from HIPAA (Cont.)

Breach:

- A breach under the HIPAA Rules is "…the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI."
- When ePHI is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy Rule.

21

Ransomware Can't Hide from HIPAA (Cont.)

Breach Notification:

- Unless the covered entity or business associate can demonstrate that there is a "…low probability that the PHI has been compromised," based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred.
- The entity must then comply with the applicable breach notification provisions, including notification to affected individuals without unreasonable delay, to the Secretary of HHS, and to the media (for breaches affecting over 500 individuals) in accordance with HIPAA breach notification requirements. See 45 C.F.R. 164.400-414
- For guidance regarding ransomware prevention and recovery see OCR Ransomware Fact Sheet on OCR website: http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

22

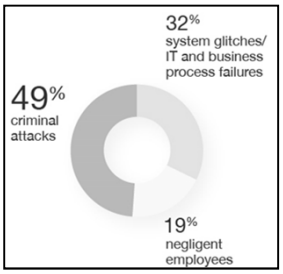
Learning Objective #4

How do we Reduce Risk

23

Understanding the Costs of Cyber-Crime

Malicious Attacks Most Costly, More Frequent



Malicious or criminal attacks include malware, criminal insiders (employees, contractors or other third parties), phishing/social engineering and web site attacks

Human error is negligent insiders that are individuals who cause a data breach because of their carelessness, as determined in a post data breach investigation.

System glitch includes loss of system or component, IT and Business process failures

24

Can we reduce the risk?

Average cost of data breach at $217 per record

- Have an incident response team - $23.8
- Extensive use of encryption - $19
- Business Continuity Management involvement - $13.6
- CISO appointed - $12.2
- Employee training - $11
- Board level involvement - $9.8
- Insurance protection - $7.9

25

Nine Steps to Reduce Your Risk

1. Annual Security Risk Assessment
2. Security Awareness Program
3. Harden Systems
4. IDS, IDP, DLP
5. Encryption
6. Vendor Management Program
7. Third-Party, Objective Review
8. Incident Response Plan
9. Cyber Insurance

26

Nine Steps to Reduce Your Risk

#1 – Annual Security Risk Assessment

- Do we Perform an Annual Security Risk Assessment?
- And do we have a program to mitigate risks identified as they change?
- Threat Intelligence

27

Nine Steps to Reduce Your Risk

#2 – Security Awareness Program

- Do we have a Security Awareness Program?
- Do we educate employees on how to handle confidential information?
- Do they know how to identify the signs?
- Does it include known risks - Social Engineering, Phishing, etc.
- Do they know who to tell?

28

Nine Steps to Reduce Your Risk

3 – Harden Systems

- Do we Harden, Update and Patch Systems?
- Does this include all systems, programs, utilities, everything?
- Baselines.
- Automated Updating.
- Ransomware Prevention
  - Provide staff with security awareness training that actively engages users to adhere to security and privacy policies
  - Tell IT ASAP – no recrimination
  - Comprehensive and regular backups
  - Antivirus with Malware detection is up-to-date
  - Disable autorun
  - Disable Windows Scripting Host (VBS)
  - Disable Remote Desktop Protocol (RDP)
  - Restrict user permissions – don't do regular work as a Sysadmin
  - Harden remote access – strong 2-factor authentication

29

Nine Steps to Reduce Your Risk

#4 – IDS, IDP, DLP

- Do we Use Intrusion Detection & Data Leak Prevention?
- Do we monitor sensitive data and control it leaving the organization?
- Do we have actionable alerts?
- And do we monitor the logs?

30

Nine Steps to Reduce Your Risk

#5 – Encryption

- Do we Utilize Encryption?
- Data at rest and in motion, websites, peripherals, email, etc.?
- HIPAA Encryption Standards
  - Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
  - Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

31

Nine Steps to Reduce Your Risk

#6 – Vendor Management Program

- Do we have a Vendor Management Program?
- Do we determine if are they "fit for purpose"?
- Vendor selection process.
- On-going monitoring.

32

Nine Steps to Reduce Your Risk

#7 – Objective Review

- Do we have experts test our system?
- Quarterly Scans
- Penetration Tests
- Internal Vulnerability Assessment
- IT Security and Controls Audit
- Do we test our websites before they go live?
- Do we follow PCI DSS for credit card handling?

33

Nine Steps to Reduce Your Risk

#8 – Incident Response Plan

- Do we have an Incident Response Plan?
- Does it include all key partners: IT, forensics, legal, PR & Management?
- Is it tested?
- Does everyone know what to do?

34

Nine Steps to Reduce Your Risk

#9 – Cyber Insurance

- Do we have Cyber Security Insurance Coverage?
  - A data breach is inevitable. Be sure to review the policy terms - Some policies exclude coverage for damages that arise out of activity that is contrary to your "Privacy Policy" … What does your Privacy Policy say exactly?
    - » if laptops are not "encrypted"
    - » for agents or vendors where there are no contracts
    - » for losses if the data is stored "in the cloud"

35

Questions

36