Understanding HIPAA Compliance

David Ashley, CISA, CISM, CBCP, CRISC, CHP
Office of the Mississippi State Auditor
Director, IT Audit Section
Tacoma, Washington NSAA IT Conference
HIPAA Compliance Audits

October 5, 2017

Bio

- 40+ years experience in IT
- 10+ years experience in Audit
- 5 Years as Director of IT Audit for MS State Auditor
- A believer in continuing education
  - MBA and ME – working toward MA in divinity
- In this business if you are not willing to accept and keep up with change you may be in the wrong business
- Blessed with 6 children (ages 15 to 37 with 3 boys the same age), as well as 7 grandchildren (age 4 and under)
"No, it's not a female Hippopotamus, anyone else know?"

HIPAA...
NOT HIPPO!!!
Large Data Breaches

- Target (40 million payment card numbers and another 70 million customer records)

- Yahoo – Over 1 billion users compromised between 2013 and 2016 (3 breaches) – Russia in 2014 -Verizon paid $4.76B for thinking they could limit liability. Federal judge ruled at end of August that Yahoo must face possible suits from those compromised.

- Equifax -143 million Americans (one-half of U.S. population) had credit records breached - CEO, CIO, and CISO all gone – Mishandled breach.

Significant State Data Breaches (Occurred in 2012, but Mitigation Ongoing)

- South Carolina Dept. of Revenue
  - ¾ of state's population
  - Cost $14M so far ($12M for credit monitoring)
  - 3.8 million instate taxpayers
  - 1.3 million out of state
  - 3 million businesses
  - 72 GB data
  - 1 month (reported by secret service)
  - **Were compliant with IRS Safeguards**
  - Will now encrypt SSN

- IRS Safeguards (Agencies that utilize IRS info)
  - MDOR, Human Services, Employment Security
**Government Hacks (2015)**

- IRS – Pulled data off IRS website to file fraudulent tax returns – Russia – Government claims NOT a hack, went in through front door (Feb. through May 2015 – $50M in fraudulent returns – 330,000 entities involved

- OPM (White House Office of Personnel Management) June 2015 – 21.5 Million records compromised – Job assignments, performance, etc.. Includes current and prior employees and individuals who applied but were not hired. Two distinct breaches 4.2M AND 18M. Since 2007 OPM notified by IG that deficiencies in cybersecurity processes. China. Nearly Year Long – Future senior government leaders and advisors could be targeted even before taking office. Could weaken the U.S. in military confrontation. Information could be given to Chinese Allies or sold by hacker.

- Joint Chief of Staff email server (Russia suspected)

- Federal Audit Clearinghouse (Anonymous in response to trade agreement)

- DNC (Democratic National Convention)

---

**Unusual Hacks**

- “Ashley Madison” – 37 Million - July 19, 2015 - 9.7G of data -
  - Touted as premiere site for married adults seeking affairs
  - 15,000 Government Employee Addresses Included
  - British government officials, United Nations employees and Vatican staff

- 1.2 Billion User Names and Passwords stolen from 420,000 websites in 2014 - Discovered by Hold Security in Milwaukee

- Deloitte Email Hack – In 2012 named best cybersecurity consult in world by Gartner. Only needed one email administrator credentials – Looked at biggest clients – Had access to 224,000 staff members on Microsoft Azure Cloud.
  - Should have had duel factor authentication (highly recommended)
Notable HIPAA Fines

- 09/22/14 - $750,000 fine for inadequate risk assessment and policies
- Alaska - Loss of Unencrypted USB Drive that may or may not have contained Protected Health Information – Fine $1.7M – 10/30/2009
- 03/16/16 - $1.55M for no HIPAA business associate agreements
- 07/16/16 – Oregon Health and Science University – widespread and diverse problems – $2.7M
- 08/04/16 – Advocate Health Care – 3 breaches involving over 4 million records - $5.5M

HIPAA Violations Close to Home (MS)

- Merit Health – Birmingham, Alabama – Involved Woman’s Hospital, River Oaks, CMMC (Central Mississippi) – Surgical Referral – Due to Employee Data Theft
- University of Mississippi Medical Center – Stolen Laptop – Fine of $2.75M – After investigation UMC found to have been in violation in several areas since 2005. FOURTH LARGEST HIPAA FINE IN HISTORY due to HIPAA violation
Possible Consequences of Non-Compliance

- Damage to or loss of data
- Damage to reputation
- Loss of customers
- Loss of debit/credit card acceptance privileges
- Breach notification costs
- Litigation costs
- Fines and incarceration
- Some HIPAA violations considered felony (willful neglect)

Examples of Consequences From Breaches Other Than Fines

- HIPAA allows fines as well as civil action by state attorney generals

- Civil action prominent with identity theft and credit card victims (Several class action suits against Ashley Madison – one $578M in Canada)

- 50 class action suits already filed against Equifax

- Providing credit monitoring is standard consequence of breach

Example: (Headlines)
- Heartland Payment Systems Enters into its Third Settlement Agreement Arising From 2008 Data Breach
Laws of the Land

- HIPAA Privacy and Security Rules (as amended by HITECH Act)
- Security Breach Notification Laws (46 States, DC, PR, and Virgin Islands)
- Payment Card Industry – Data Security Standard
- Federal Trade Commission – Red Flags Rule
- Federal Trade Commission – Disposal Rule
- Federal Information Security Management Act of 2002
- Multiple Federal Privacy Bills Introduced Each Year
- Whitehouse Consumer Privacy Bill of Rights (February 2012)

Data Security Issues and Data Breach Notification

- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Part 2 – Confidentiality of Alcohol and Drug Abuse Patient Record Regulation
- Sarbanes Oxley
- State Laws and Regulations
- Section 5 of FTC Act for companies who store consumer information on the cloud
International Laws

  - Some information of residents of EU cannot be stored outside the EU
- Australia’s Privacy Laws
- Canada’s Privacy Laws

Compelled Disclosure to the Government

- Electronic Communications Privacy Act (ECPA)
- Stored Communications Act (SCA)
- USA Patriot Act (including National Security Letters; FISA warrants)
- Warrants and Subpoenas Generally - eDiscovery
Data Security Issues – Federal Laws, Regulations and Standards

- Federal Laws and Regulations:
  - Healthcare (HIPAA and HITECH)
  - Educational institutions (FERPA)
  - Financial institutions (GLBA)
  - Publicly traded companies (SOX)
- Entities cannot generally contract away its obligations to comply with these
- Some regulations, however, require an entity to pass obligations to cloud providers by contract (e.g., HIPAA)

State Data Breach Laws

- 47 States, DC, Puerto Rico, Guam, and Virgin Islands
- States that don’t have include New Mexico, South Dakota, and Alabama
- Mississippi (75-24-29) enacted July 1, 2011
- Name or first initial and last name in combination with any one or more of the following data elements: Social security number; Driver's license number or state identification card number; or an account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual’s financial accounts (Several cross foot websites)
Forthcoming Guidelines

- FTC – Federal Trade Commission or Law on Oversight of PII, especially credit information where no consent involved. Investigating SEC and Equifax.
- SOC for Cybersecurity (AICPA) – Reporting format
- AICPA also offering certification in cybersecurity
- State Cybersecurity Laws (Stipulating Responsibilities of Various State Entities (i.e. MS House Bill 999)
- Publication 100 – Dept. of Commerce – Death Master

New Technology, New Risks

- Flash Drives, Memory Cards, and other Removable Media
- I-Pods, MP3 players, Digital Cameras
- Smart Devises: Cell phones, PDAs, Tablets
- Instant Messaging, Text Messaging, Media Messaging
- Remote Access: (BYOD) employees, vendors, clients
- Wireless Networks: work and home
- Voice over Internet Protocol (VoIP), Unified Messaging
- Storage Area Networks, Electronic Data Vaulting
- PC Virtualization, Server Virtualization
- Software as a Service (SaaS), Cloud Computing
- Infrastructure as a Service (IAS)
- Advanced Persistent Threats (APTs)
- Cloud Computing and Storage
- Facebook
- Twitter
- Snapchat
Development of Today’s Attack Continuum

- PC virus appeared more than 25 years ago
- For nearly 10 years, viruses endured as primary method of attack.
- Approximately every 5 years attackers would launch new types of threats
- Today we are faced with advanced malware, targeted attacks and advanced persistent threats (APTs)
- Difference in this era from the past are motivations and the tools behind the attacks, making them particularly challenging to detect, understand and stop.

Addressing Sooner Than Later

- Recognize that:
  - Most security tools today focus on providing visibility into network and blocking malware at the point of entry.
  - Advanced attacks now employ tactics such as port hopping, encapsulation, zero-day attacks, sleep techniques, encrypted traffic, and sandbox evasion.
  - If file is not caught or it evolves and becomes malicious after entering environment, point-in-time detection technologies cease to be useful.
On black market (dark internet):
- Credit card info worth about 50 cents
- Social Security Number worth about $15
- Medical record information worth about 60 dollars
- One-third of all cases of identity theft is medical identity theft
- In 2015 almost 100 million healthcare records compromised making healthcare records the #1 target for hacking

Responding to Possible Attack
- Detach from network (wire and wireless)
- No emails out or in
- Report ASAP to Security Officer
- Don’t open attachments from places you don’t know
**Signs of Infection**

- Slow machine
- Browser doing funny stuff
- Popups
- Unexpected Sounds
- Going to Random Sites
- Files or Folders Deleted or Changed

---

**HIPAA**

**Covered Entity vs Business Associate**

- What are the differences between them:
- Covered Entities as defined by HHS and required by Congress to comply with HIPAA are:
  - Health plans
  - Health care clearinghouses
  - Health care providers conducting certain financial and administrative transactions electronically.
- Business Associates are:
  - Contracted by Covered Entities to perform work involved with HIPAA related information.
Applies To
All HIPAA Covered Entities

- Health Plans
- Health Care Clearinghouses
- Health Care Providers who conduct electronic transactions, not just those who accept Medicare or Medicaid
  - Any provider who accepts payments from any health plan or other insurance company must comply with HIPAA if they conduct the adopted transactions electronically.

HIPAA Security Standards
What is “PII”?

- “Personal Identifiable Information” – information that includes an individual’s name in combination with any one or more of the following:
  - Social Security Number
  - Driver’s license number
  - State-Issued ID card #
  - Credit / debit card number in combination with their access / security code or password
**HIPAA Security Standards**

**What is “PHI”?**

Individually Identified Health Information that is collected from the Beneficiary or created or received by a Covered Entity that relates to:

- Physical/mental health or condition of an individual, or
- Provision of healthcare, or
- Payment for the provision of healthcare, AND
- Could potentially identify an individual

Excludes education records under FERPA

Excludes employment records held by a CE as employer

**HIPAA Security Standards**

**What constitutes PHI – Eighteen identifiers**

- Name
- Address -- street address, city, county, zip code (more than 3 digits) or other geographic codes
- Dates directly related to beneficiary
- Telephone Number
- Fax Number
- Email Addresses
- Social Security Number
- Medical Record Number
- Health Plan Beneficiary Number
- Account Number
- Certificate/License Number
- Any vehicle or device serial number
- Web URL
- Finger or voice prints
- Photographic images
- Internet Protocol (IP) Address
- Any other unique identifying number, characteristic, or code (whether generally available in the public realm or not)
- Age greater than 89 or any other demographics that create a relatively small population
ePHI: data in an electronic format that contains any of the 18 identifiers

This may include but is not limited to the following:

- Data stored on the network, internet, or intranet
- Data stored on a personal computer or personal digital assistant i.e. Palm Pilot or SmartPhone
- Data stored on “USB keys,” memory cards, external hard drives, CDs, DVDs, floppy disks, tapes, or digital cameras/camcorders
- Data utilized for reporting
- Data in electronic communications

Multiple types of PHI and ePHI adds to the importance of Business Associate Agreements (BAAs)

What are some examples of PHI for OSA auditors?

- Protected E-mail communications related to health care for a beneficiary
- A care plan for a beneficiary FAXed by a care provider to an OSA employee
- Slides of beneficiaries where the beneficiary can be identified
HIPAA and HHS, CMS, OCR

- **HHS – Health and Human Services** - The U.S. government’s principal agency for protecting the health of all Americans and providing essential human services. Responsible for 25% of outlays of government and administers more grants than all other agencies combined.

- **CMS – Centers for Medicare and Medicaid Services**
  The Centers for Medicare & Medicaid Services (CMS) is a federal agency within HHS that administers the Medicare program and works in partnership with state governments to administer Medicaid, and health insurance portability standards. In addition to these programs, CMS has other responsibilities, including the administrative simplification standards from the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- **OCR – Office for Civil Rights**
  Through the federal civil rights laws and Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, OCR protects your fundamental nondiscrimination and health information privacy rights.

The History of HIPAA

- August 1996 – HIPAA Introduced
- August 1998 – Security and Electronic Signature Standards Rule
- April 2003 – HIPAA Privacy Rule Compliance Deadline
- October 2003 – Transactions and Code Sets Rule Deadline
- April 2005 – HIPAA Security Rule Compliance Deadline
- March 2006 – Enforcement Rule Goes Into Effect
- December 2012 – OCR Begins HIPAA Compliance Audits
- 2015 & Beyond – This year the OCR is due to complete the delayed second round of HIPAA compliance audits
HIPAA Security Standards

What is HIPAA?

HIPAA refers to the:

Health Insurance Portability and Accountability Act of 1996

- HIPAA is a Federal law
- HIPAA establishes certain minimum federal standards. Generally, state laws which are more strict than HIPAA will still apply

HIPAA Security Standards

What is HIPAA meant to do?

- Allow people to move their health insurance coverage when they change or lose their jobs
- Reduce health care fraud and abuse
- Establish standards for Administrative Simplification
  - To promote electronic health care transactions
  - To streamline medical claims processing
- Protect Beneficiary Information - PRIVACY
HIPAA was not designed to restrict access to personal health information for OSA employees who need that information to provide care.

- HIPAA was designed to make sure that systems, policies and procedures are in place to protect individually identifiable information from unnecessary disclosure.
HIPAA Security Standards
How does HIPAA insure privacy?

- Defines Protected Health Information (PHI)
- Defines who may see or use health information and what they can do with it
- Limits many uses and disclosures of health information to the “minimum necessary” amount needed for the task
- Establishes new beneficiary rights concerning their health information

HIPAA Security Standards
Privacy – In Summary

- Keep Protected Health Information private and secure at all times
- Make sure only personnel who need to use Protected Health Information see it or use it
- Use only the minimum amount of Protected Health Information necessary to accomplish the task
- Read and understand Privacy policies and procedures
- Know your Privacy Officer and Security Officer
- Consult your Security with any questions you have about Protected Health Information
HIPAA Security Standards

What is the Security Rule?

Legislation designed to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI).

Comprised of three main categories of “standards” pertaining to the administrative, physical, and technical aspects of ePHI.

Applies to the security and integrity of electronically created, stored, transmitted, received, or manipulated personal health information.

OMNIBUS FINAL RULE

HIPAA & HITECH Changes
Omnibus Rule Modifications

- HIPAA
  - Privacy
  - Security
  - Enforcement
- HITECH
  - Breach Notification
- Genetic Information Nondiscrimination Act (GINA) of 2008

Investigation – §160.306

- Secretary will investigate any complaint when a preliminary review of the facts indicates possible violation due to willful neglect
- Secretary will conduct a compliance review when a preliminary review of the facts indicates possible violation due to willful neglect
- An investigation under this section may include a review of the pertinent policies, procedures, or practices of the covered entity or business associate and of the circumstances regarding any alleged violation
- At the time of the initial written communication with the covered entity or business associate about the complaint, the Secretary will describe the acts and/or omissions that are the basis of the complaint
- OCR currently conducting Phase II of HIPAA Audit Program
Civil Money Penalties – §160.404

- $100 – $50,000 – did not know and would not have known
- $1000 – $50,000 – reasonable cause to know
- $10,000 – $50,000 - willful neglect, timely corrected (30 days)
- $50,000 – willful neglect NOT corrected
- $1.5 million cap for identical violations during a calendar year

- **Reasonable cause** – knew, or by exercising reasonable diligence would have known, the act or omission was a violation, but did not act with willful neglect
- **Willful neglect** – conscious, intentional failure or reckless indifference to the obligation to comply

Notification of Breach

- **To Individuals**
  - ✓ Must notify without unreasonable delay
  - ✓ No later than 60 calendar days after discovery of a breach

- **To HHS**
  - ✓ 500 or more individuals
    - ✓ Must notify without unreasonable delay
    - ✓ No later than 60 calendar days after discovery of a breach
  - ✓ Less than 500 individuals
    - ✓ Notify no later than 60 days after the end of the calendar year in which the breaches were “discovered,” not in which the breaches “occurred”
**Business Associate – §160.103**

- **Old definition**
  - Performs or assists in performance of a function or activity

- **New definition**
  - Creates, receives, maintains, or transmits PHI for a function or activity
  - **Includes**
    - A health information organization, e-prescribing gateway, or other entity that provides data transmission services and requires ongoing access
    - An entity that offers a personal health record on behalf of the covered entity
    - A subcontractor that creates, receives, maintains, or transmits PHI on behalf of BA

---

**Liabilities for Business Associates and Subcontractors**

- **Privacy Rule**
  - If the BA is to carry out the covered entity’s obligations under the Privacy Rule, the business associate must comply with the requirements of the Privacy Rule that apply to the covered entity in the performance of such obligations

- **Security Rule**
  - BA is directly subject to the Security Rule

- **Must have comprehensive HIPAA policies and procedures**

- **BAA with Subcontractor**
  - BA must enter into a BAA with subcontractors to whom the BA has delegated a function, activity, or service the BA has agreed to perform for a covered entity, and such function, activity, or service involves the creation, receipt, maintenance, or transmission of PHI
HIPAA Security Standards
Specific Ways Staff Can Help

- Assure the access to ePHI and PHI is appropriate
- Manage your password
- Be aware of physical security
- Use equipment properly / use device controls
- Make sure portable devices are secure
- Manage data properly (PHI and ePHI)
- Identify and keep out malicious software
- Manage e-mail properly
- Use the Internet safely
- Learn and follow our policies and procedures

HIPAA Security Standards
Security for Portable Devices & Laptops with ePhi

- Implement the workstation physical security measures listed for Workstation Security, plus this Check List
  - Use up-to-date Anti-virus software
  - Install computer software updates, e.g., Microsoft patches
  - Encrypt and password protect portable devices
  - Lock-it up!, e.g., Lock office or file cabinet, lock up laptops
  - Automatic log-off from programs
  - Use password protected screen savers
  - Back-up critical data and software programs
Remember privacy guidelines and apply them to physical and electronic data.

- Password protect and encrypt data when needed.
- Encrypt all ePHI that travels outside entity’s trusted network.

Workforce members who violate policies regarding privacy / security of confidential, restricted and/or protected health information or ePHI are subject to further corrective and disciplinary actions according to existing policies.

- Actions taken could include:
  - Termination of employment
  - Possible further legal action
  - Violation of local, State and Federal laws may carry additional consequences of prosecution under the law, costs of litigation, payment of damages, (or both); or all.
  - Knowing, malicious intent → Penalties, fines, jail!
Office of the State Auditor
HIPAA Compliance Training

"We need to review our training material."

Thank You

David Ashley,
Office of the State Auditor
P.O. Box 956
Jackson, MS 39205
david.ashley@osa.ms.gov
Web: www.osa.ms.gov