MURTHA CULLINA

Cyber (In)Security:
Cyber Attacks, Breaches and HIPAA Compliance

Dena M. Castricone, Esq., CIPP/US
203-772-7767| dcastricone@murthalaw.com

October 27, 2017

Cyber Threats in Health Care

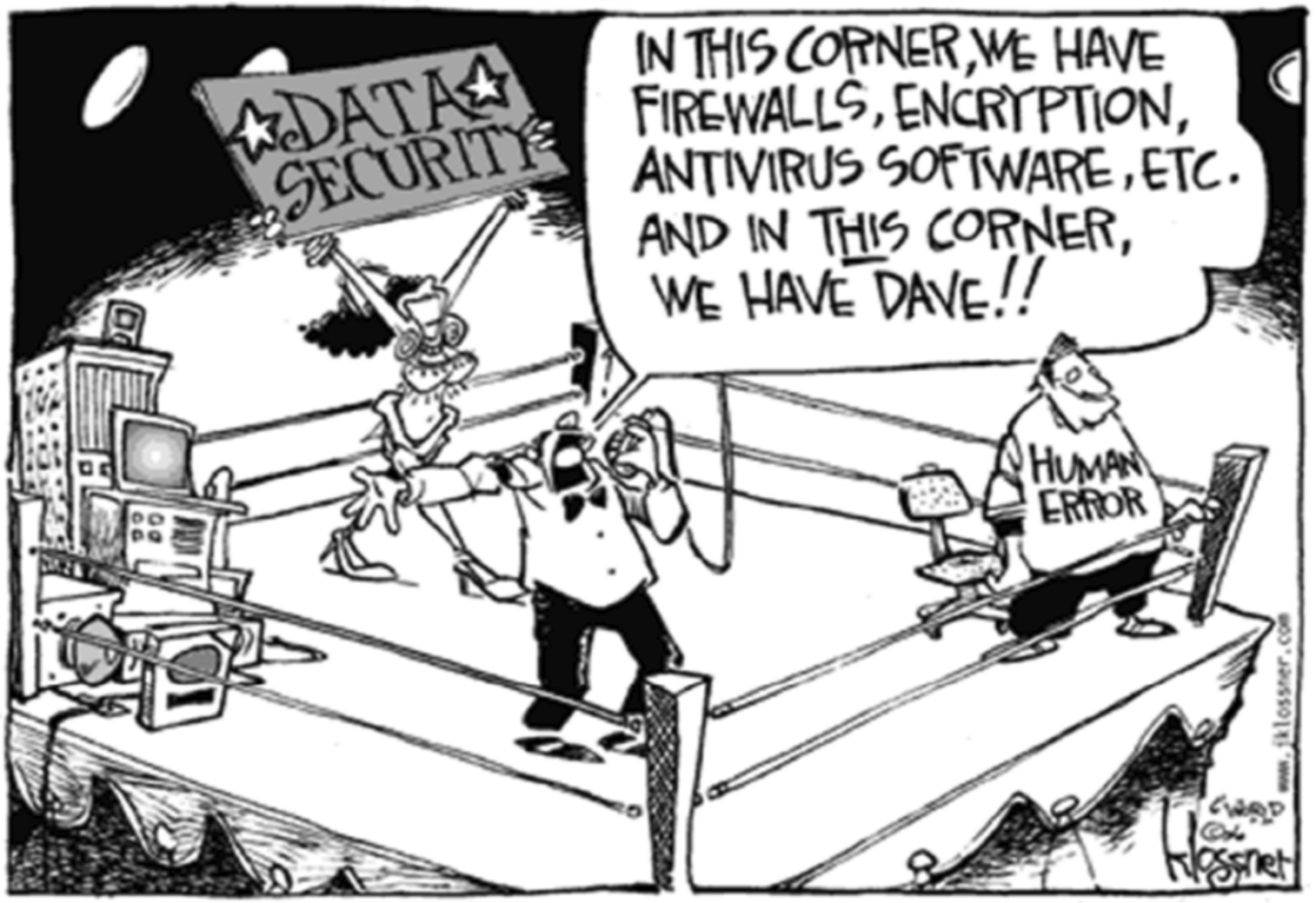
- 202 breaches reported to OCR involving < 500 patients
  - 3,978,733 total records impacted
  - 93 of the 202 (46%) categorized as Hacking/IT incident
  - 2,849,264 records in those 93 incidents (71% of total)

Cyber Threats in Health Care

- Cost of health care data breach: $380 per record
  - As compared to $225 per record in other industries
- Experian 2017 report: “medical identity theft remains lucrative and easy for cyber criminals”
- Health care is a target because:
  - Limited spending in cyber security
  - High demand for health records on dark web

Cyber Threats in Health Care

- Multiple studies agree that phishing emails are the most common distribution method for malware (including ransomware): 67% to 91%
  - Train employees about phishing emails
  - The best detection systems cannot keep your employees from clicking on links or opening attachments


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
Klossner

Cyber Threats in Health Care

- Ransomware
  - 50% of data security incidents from Oct. 2015 to Sept. 2016 caused by healthcare ransomware attacks
- Ransomware continues as top concern
- Networked and mobile medical devices growing concern

New Ransomware Threat

- In late August, information was released about a new strand of ransomware called “Defray” targeting healthcare institutions
  - Distributed in small email campaigns using messages from the IT director and including the institution’s logo
  - The attached document purports to be patient reports detailing important information for patients, relatives and caregivers
  - Opening document will unleash ransomware for which there is no free decryption key; must pay the $5,000 ransom or rely on backups

Recent Medical Device Threats

- (Aug. 29) FDA announced firmware update to pacemakers vulnerable to cyber security attacks
  - If exploited, could allow access to device using commercially available equipment (465,000 devices)
- (Aug. 3) Siemens identified four vulnerabilities within its Molecular Imaging products running on Windows 7 (PET scan and other devices)

Cyber Attacks Cause HIPAA Breaches

- Under HIPAA, a breach is any impermissible use or disclosure that compromises the security or privacy of the PHI
  - A breach is presumed unless the CE or BA demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment

OCR Guidance on Ransomware

- Issued in 2016; reissued in May 2017
- "When electronic protected health information (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." (emphasis added)

OCR Guidance on Ransomware

- While OCR's statement seemingly is definitive about ransomware and breach, it does note that a breach is presumed to have occurred 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…"

OCR Cybersecurity Checklist

- OCR issued a checklist outlining steps for providers to take in the event of a cybersecurity incident
- This checklist should be consulted in creating/updating an incident response plan
- It assumes that providers already have certain contingency and backup plans in place

OCR Cybersecurity Checklist

- Must execute its response and mitigation procedures and contingency plans
  - Immediately fix any technical or other problems to stop the incident
  - Take steps to mitigate any impermissible disclosure of PHI
- Should report the crime to other law enforcement agencies

OCR Cybersecurity Checklist

- Should report all cyber threat indicators to federal and information-sharing and analysis organizations (ISAOs)
  - the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response, and private-sector cyber-threat ISAOs
- Must report the breach to OCR as soon as possible, but no later than 60 days after the discovery of a breach affecting 500 or more individuals

HIPAA Enforcement is Up

- Jan. – April 2017 – OCR entered into 7 settlements with fines totaling more than $14 million
- 2016 – more than $23.5 million in fines (a record-breaking year – up 300% from previous years)
- Large and small providers at risk
- Even FQHCs have been hit with sizable fines

OCR Enforcement

- April 2017 – An FQHC experienced a breach due to a phishing incident in 2012. While the FQHC took corrective action, OCR's investigation exposed that the FQHC failed to conduct its first risk analysis until mid-February 2012, weeks after the incident.
- OCR settlement: $400,000

Recent OCR Reports (July and August)

- Delaware-based oncology provider suffered a ransomware attack potentially impacting PHI of 19,203 patients
  - hackers targeted electronic files on server and workstations as early as June 17 but not discovered until July 7
- Pacific Alliance Medical Center hit by a ransomware attack, potentially breaching protected health information of 266,123 patients
  - could not determine whether data was viewed or stolen

Recent OCR Reports (July and August)

- New York's largest provider notified patients of a phishing incident that impacted 744 patients
  - hacker gained access to an employee's email account and accessed a "small number of Kaleida Health email accounts"
- St. Mark's Surgery Center hit by a ransomware attack that may have impacted the PHI of 33,877 patients
  - prevented patient data from being accessed for three day period
  - investigation was inconclusive as to whether PHI was viewed or stolen, therefore, the provider reported

Recent OCR Reports (July and August)

- The Women's Health Care Group of Pennsylvania notified 300,000 patients of a ransomware attack
  - The investigation revealed the cybercriminals began hacking the system as early as January 2017
- Plastic Surgery Associates of South Dakota hit by a ransomware attack possibly impacting PHI of 10,200 patients
  - The hackers unable to access the majority of medical data but officials lost evidence of lack of access during cleanup; therefore had to report

Mitigating the Risk

- Risk of cyber threats can be substantially limited by:
  - Assessment of systems for areas of risk
  - Employee training
  - Adequate security policies
  - Adequate security measures

All are required by HIPAA Security Rule

Mitigating the Risk – HIPAA Security Rule

- Ensure the confidentiality, integrity, and availability of ePHI
- Protect against reasonably anticipated:
  - threats or hazards to ePHI
  - unauthorized uses or disclosures
- Ensure compliance by workforce

Security Rule

- 45 CFR 164.308 – most of the relevant security standards. The three sections below will be helpful in mitigating cybersecurity risk:
  1. Security Management Process – 164.308(a)(1)
  2. Security Awareness Training – 164.308(a)(5)
  3. Contingency Plan – 164.308(a)(7)

Security Rule – Required and Addressable

- All implementation specifications are either “required” or “addressable”
  - “required” components must be implemented
  - “addressable” components must be assessed to determine if the specification is reasonable and appropriate
- Specific measures used will vary depending on size, complexity and capability

#1 - Security Management Process

- Standard: Implement policies and procedures to prevent, detect, contain, and correct security violations
- Implementation specifications (all required):
  - Risk analysis
  - Risk management of known risks
  - Sanction policy
  - Audit system activity

#1 - Security Management Process

- Risk analysis
  - Assessment of the potential risk and vulnerabilities to the confidentiality, integrity and availability of PHI
  - Area of focus of OCR on audits and investigations
  - Must be comprehensive
  - Can be done internally or can use a vendor
    - If using a vendor, select wisely

#1 - Security Management Process

- Risk management of known risks
  - Implement measures to reasonably reduce risks identified in the analysis
  - Cannot eliminate risk
  - Key is reducing to a reasonable and appropriate level
  - Must at least address every finding in the analysis

#1 - Security Management Process

- Sanction policy
  - Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures
- Audit system activity
  - Implement procedures to regularly review records of information system activities
    - Audit logs, access reports and incident tracking reports

#2 - Security Awareness Training

- Standard: Implement a security awareness and training program for all members of its workforce
- Implementation specifications (all addressable):
  - Security reminders
  - Protection from malicious software
  - Log-in monitoring
  - Password management

#2 - Security Awareness Training

- All implementation specifications are “addressable”
  - “addressable” components must be assessed to determine if the specification is reasonable and appropriate
- Given the current state of cybersecurity issues in health care, implementing each of these specifications on some level is advisable

#2 - Security Awareness Training

- Security reminders (addressable)
  - Periodic security updates
  - E.g. monthly emails about current risks including phishing attacks, common malware sources, etc.
- Protection from malicious software (addressable)
  - Procedures for guarding against, detecting, and reporting malicious software
  - Anti-virus software, system patches, monitoring efforts

#2 - Security Awareness Training

- Log-in monitoring (addressable)
  - Procedures for monitoring log-in attempts and reporting discrepancies
- Password management (addressable)
  - Procedures for creating, changing, and safeguarding passwords
  - Having a password policy that requires strong passwords and prohibits password sharing

#3 - Contingency Plan

- Standard: Establish P&P for responding to an emergency or other occurrence that damages systems containing PHI
- Implementation specifications:
  - Data Backup Plan
  - Disaster Recovery Plan
  - Emergency Mode of Operation Plan
  - Testing and Revisions Procedures
  - Applications and Data Criticality Analysis

#3 - Contingency Plan

- Data Backup Plan
  - Procedures to create and maintain retrievable exact copies of ePHI
  - One of the most important tools in mitigating damage from a cyberattack
  - Ensure that backups are maintained separate from the network so they are not impacted by an attack
  - Periodically test backups

#3 - Contingency Plan

- Disaster Recovery Plan
  - Procedures to restore any loss of data
- Emergency Mode of Operation Plan
  - Procedures to enable continuation of critical business processes for the protection of PHI while operating in emergency mode
- Testing and Revisions Procedures (addressable)
  - Periodic testing and revision of contingency plans
- Applications and Data Criticality Analysis (addressable)
  - Assess criticality of specific applications and data in support of other contingency plan components

Highlights of Standards

- Assess the potential risks and vulnerabilities and address those identified risks
- Train, train, train (and test knowledge – consider simulated phishing attacks or other training tools)
- Back up your data often and keep backup separate from the main network. Also, practice response to a cyber attack situation.

NIST Framework

- Identify, Protect, Detect, Respond and Recover
- 22 categories and 98 subcategories under those five functions
- Framework for Improving Critical Infrastructure Cybersecurity is out in draft; finalized next year

NIST Framework

- Resulted from a 2013 executive order calling for a set of industry standards and best practices to manage cybersecurity risk
- Helpful tool in creating cybersecurity strategy
- Draft: https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf


KAL
Q.
WHAT WILL THE WARRIOR-GUARDIAN OF THE FUTURE LOOK LIKE?
Yo! DUDE... BACK HERE
CYBER SECURITY