Cyber Security In Healthcare

John DiMaggio, C.E.O., Blue Orange Compliance

BLUE ORANGE® COMPLIANCE

HIMSS® CENTRAL & SOUTHERN OHIO *Chapter*

About the Presenters

John DiMaggio, Chief Executive Officer, Blue Orange Compliance

John DiMaggio is the co-founder and CEO of Blue Orange Compliance, a firm dedicated to helping health care providers and business associates navigate the required HIPAA and HITECH Privacy and Security regulations. John is a recognized healthcare information compliance speaker to state bar associations, HIMSS, Health Care Compliance Association (HCCA) and long term care associations including Long Term and Post Acute Care (LTPAC), NAHC, LeadingAge and ALFA. John is also a LeadingAge CAST Commissioner.

John's extensive healthcare experience includes Chief Information Officer with NCS Healthcare and Omnicare; senior operations roles with NeighborCare, and general consulting to the industry. John began his career as a key expert in Price Waterhouse's Advanced Technologies Group and served on several national and international standards organizations including the American National Standards Institute (ANSI) and the International Standards Organization (ISO).

John is the named inventor for multiple healthcare technology and process patents. He holds an MBA in Finance from Katz Graduate School of Business and a BS in Computer Science from the University of Pittsburgh.

About Blue Orange

Specialize in healthcare information privacy and security solutions.

Columbus-Based

National Provider

We understand that each organization is busy running its business and that human capital is limited. Our high-tech, low-touch, cost-effective approach provides continuous, maximum information and guidance and requires minimal staff time and engagement.

- Security Risk Assessments and Guidance
- HIPAA Privacy and Security
- Penetration testing
- Mock Office for Civil Rights HIPAA Audits
- Analytics

Agenda

- Overview
- Breaches
- Risk
- Cyber Criminal Techniques
- Prevention
- Preparation/Response - “It’s not if, it’s when”
- Governance

Healthcare Landscape

Healthcare

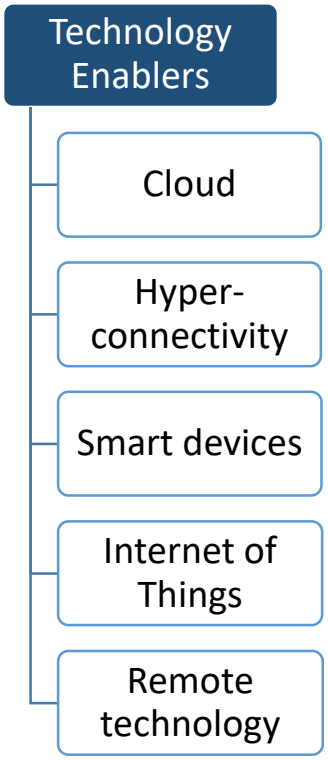
- Electronic
- Push toward interoperability
- Cost shift outside 4 walls
- Information outside 4 walls

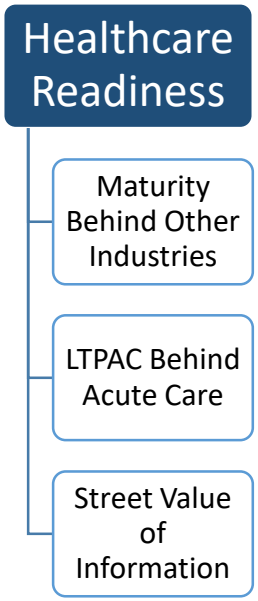
Acute Care

- EHR start since 2010
- Meaningful Use Stages
- Receiving incentives

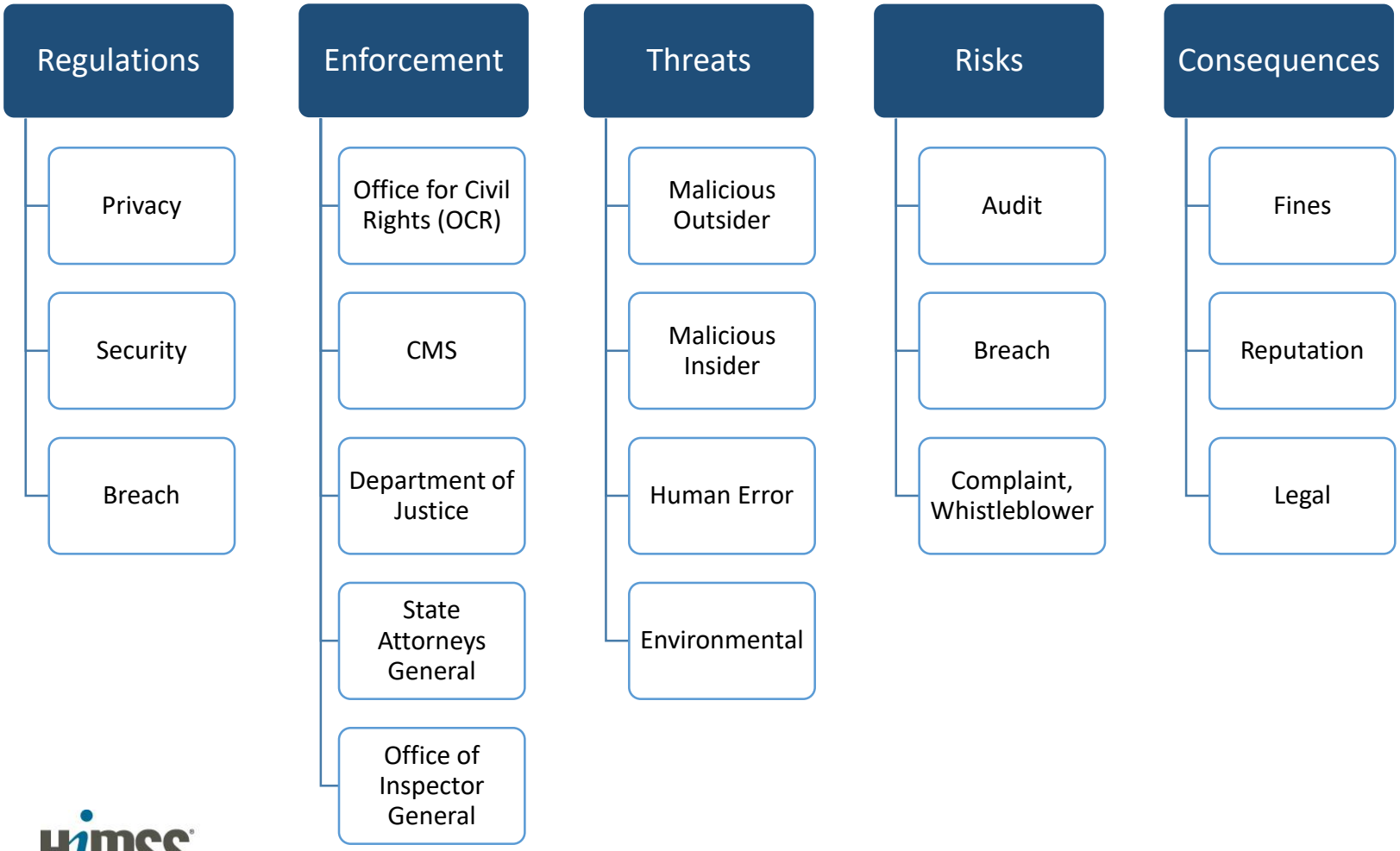
Long Term Post-Acute Care (LTPAC)

- Push toward interoperability
- Implementing EHR
- Implementing applicable technology

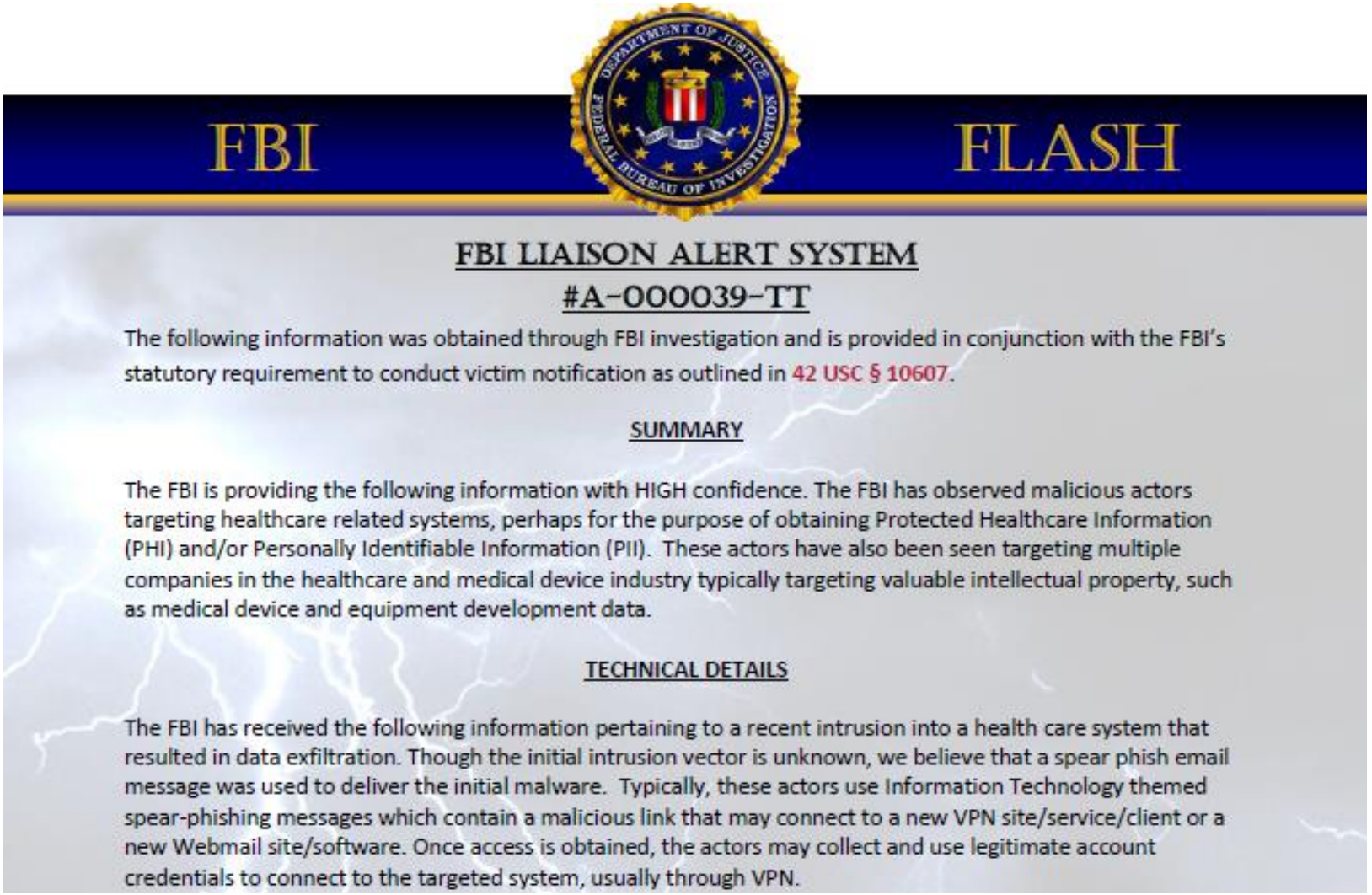




Privacy and Security



HIMSS CENTRAL & SOUTHERN OHIO Chapter



FBI FLASH

FBI LIAISON ALERT SYSTEM
#A-000039-TT

The following information was obtained through FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in 42 USC § 10607.

SUMMARY

The FBI is providing the following information with HIGH confidence. The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII). These actors have also been seen targeting multiple companies in the healthcare and medical device industry typically targeting valuable intellectual property, such as medical device and equipment development data.

TECHNICAL DETAILS

The FBI has received the following information pertaining to a recent intrusion into a health care system that resulted in data exfiltration. Though the initial intrusion vector is unknown, we believe that a spear phish email message was used to deliver the initial malware. Typically, these actors use Information Technology themed spear-phishing messages which contain a malicious link that may connect to a new VPN site/service/client or a new Webmail site/software. Once access is obtained, the actors may collect and use legitimate account credentials to connect to the targeted system, usually through VPN.

Federal Bureau of Investigation. FBI Liaison Alert System #A-000039-TT, August 19, 2014

Top 10 Healthcare Breaches 2016

1. Banner Health (Phoenix). In the largest data breach of 2016, 3.7 million patients, Banner health plan members and beneficiaries and food and beverage customers and providers were affected.

2. Newkirk Products (New York City). Newkirk Products, which issues ID cards for health insurance plans, including a number of Blue Cross Blue Shield plans, reported a data breach affecting 3.3 million individuals.

3. 21st Century Oncology (Fort Myers, Fla.). In March, the cancer care services provider reported a data breach that occurred in October 2015 and affected 2.2 million individuals, according to Health Data Management.

4. Valley Anesthesiology and Pain Consultants (Phoenix). In August, the clinic began notifying patients, employees and providers of a breach that affected 882,590 individuals.

5. Bon Secours Health System (Marriottsville, Md.). Approximately 655,000 patients were affected after a vendor inadvertently left patient information accessible on the internet.

6. Peachtree Orthopaedic Clinic (Atlanta). The clinic reported the breach, which affected 531,000 individuals, this fall.

7. Radiology Regional Center (Fort Myers, Fla.). Patient records from the center fell off the back of a waste management truck in December 2015. Approximately 483,063 individuals were affected, according to Health Data Management.

8. California Correctional Health Care Services (Elk Grove). CCHCS, a provider of healthcare to adult inmates in the state, reported a data breach after a laptop was stolen from an employee's car. Approximately 400,000 individuals were affected, according to Health Data Management.

9. Community Health Plan of Washington (Seattle). A data breach affected 381,534 current and former members of the health plan, which provides insurance to Washington's Medicaid members.

10. Central Ohio Urology Group (Gahanna). An August cyberattack on Central Ohio Urology Group affected 300,000 patients.

11. Premier Healthcare (Bloomington, Ind.). The multispecialty physician group notified more than 200,000 patients of a data breach that stemmed from a stolen laptop.

Ponemon Statistics

Cyber criminal attacks as root cause of breaches:

- **Breaches experienced in last 2 years: 50%**
- **2015: 45%**
- **2011: 20%**

Next leading cause: Error by 3rd party partner (Business Associate)

Average number of days before a breach is detected: 201 days

Source: Ponemon Institute: Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data

Cyber Security: Immutable Truths

"There are some fairly simple, immutable truths that each of us should keep in mind, truths that apply equally to political parties, organizations and corporations alike:

- If you connect it to the Internet, someone will try to hack it.
- If what you put on the Internet has value, someone will invest time and effort to steal it.
- Even if what is stolen does not have immediate value to the thief, he can easily find buyers for it.
- The price he secures for it will almost certainly be a tiny slice of its true worth to the victim.
- Organizations and individuals unwilling to spend a small fraction of what those assets are worth to secure them against cybercrooks can expect to eventually be relieved of said assets."

Source: Krebs on Security -DNI: Putin Led Cyber, Propaganda Effort to Elect Trump, Denigrate Clinton. Jan 17

HIPAA Breach Definition

"The acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E ("HIPAA") which compromises the security or privacy of the protected health information."

HIPAA – Who needs to comply?

- Covered Entity (CE):
  - Health Plans
  - Health Care Providers: Any provider who electronically transmits health information in connection with standardized transactions regulated by HIPAA (e.g., claims transactions, benefit eligibility inquires, etc.).
  - Health Care Clearinghouses: Entities that process nonstandard information they receive from one entity into a standard format (or vice versa).
- Business Associate (BA):
  - A person or organization (other than a member of the CE's workforce) that performs certain functions or activities on behalf of the CE that involves the use or disclosure of protected information.
- HIPAA Entity Types
  - Covered Entity
  - Affiliated Covered Entity (ACE)
  - Hybrid
  - Organized Healthcare Arrangement (OHCA)

Regulations

- HIPAA (Federal floor)
  - 45 CFR 164 Subpart C - **SECURITY** STANDARDS FOR THE PROTECTION OF ELECTRONIC PROTECTED HEALTH INFORMATION
  - 45 CFR 164 Subpart E - **PRIVACY** OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION
  - 45 CFR 164 Subpart D - NOTIFICATION IN THE CASE OF **BREACH** OF UNSECURED PROTECTED HEALTH INFORMATION

- State Regulations
  - Confidentiality
  - Patient Rights
  - Breach

What's at Risk? Penalties Plus…

Civil Monetary Penalties

Willful Neglect <u>not</u> corrected within 30 days	• Min. $50,000/violation • Max. $1,500,000/ calendar year
Willful Neglect corrected within 30 days	• Min. $10,000/violation • Max $50,000/violation • Max. $1,500,000/ calendar year
Reasonable Cause	• Min. $1000/violation • Max $50,000/violation • Max. $1,500,000/ calendar year
Did not Know	• Min. $100/violation • Max $50,000/violation • Max. $1,500,000/ calendar year

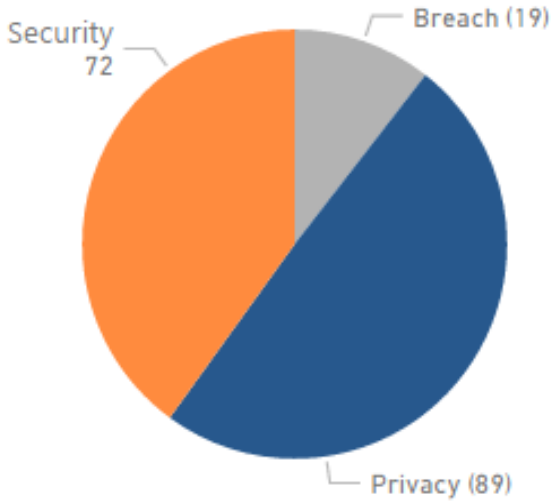
Other Costs

- Legal
- Accelerated Remediation
- Public Relations
- Reputation

US Department of Health and Human Services Office for Civil Rights. 45 CFR 160.404

Office for Civil Rights HIPAA Audit Protocol

180 Audit Items



General Item Structure

1. Do Policies and procedures exist for the item?
2. Does the entity perform the necessary requirements for the item?
3. Obtain and review policies and procedures for the item and ensure they have required elements
4. Obtain and review documentation demonstrating the item is being performed in accordance with policies and procedures

OCR Audit Protocol Walkthrough

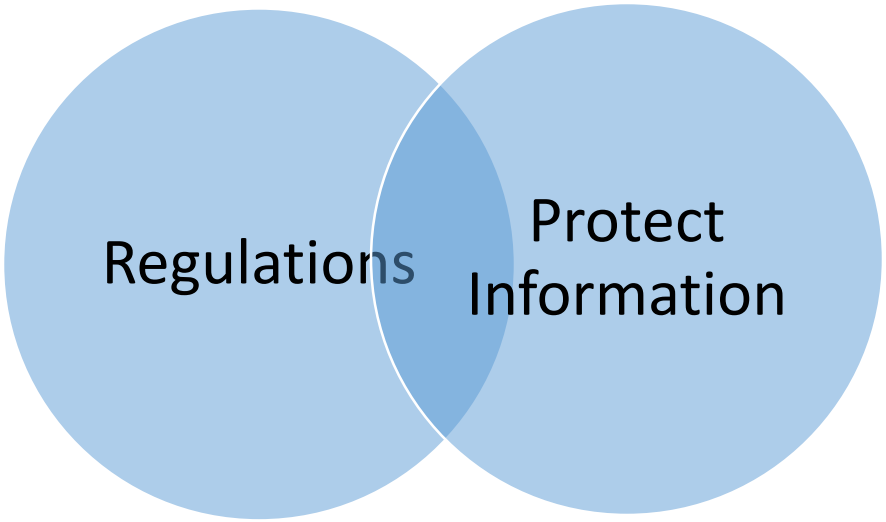
Security Example

Audit Type	Section	Key Activity	Established Performance Criteria	Audit Inquiry
Security	§164.308(a)(1)(ii)(A)	Security Management Process -- Risk Analysis	§164.308(a)(1)(ii)(A): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.	Does the entity have policies and procedures in place to conduct an accurate and thorough assessment o the confidentiality, integrity, and availability of all the electronic protected health information (ePHI) it creat Has the entity conducted an accurate and thorough assessment of the potential risks and vulnerabilities t availability of all the ePHI it creates, receives, maintains, or transmits? Determine how the entity has implemented the requirements. Obtain and review risk analysis policies and procedures. Evaluate and determine if written policies and pr the purpose and scope of the risk analysis, workforce member roles and responsibilities, management inv frequently the risk analysis will be reviewed and updated. Obtain and review the written risk analysis or other record(s) that documents that an accurate and thorou vulnerabilities to the confidentiality, integrity, and availability of all ePHI was been conducted. Evaluate an other documentation contains: • A defined scope that identifies all of its systems that create, transmit, maintain, or transmit ePHI • Details of identified threats and vulnerabilities • Assessment of current security measures • Impact and likelihood analysis • Risk rating Obtain and review documentation regarding the written risk analysis or other documentation that immedia or other record, if any. Evaluate and determine if the risk analysis has been reviewed and updated on a pe the environment and/or operations, security incidents, or occurrence of a significant event.
Security	§164.308(a)(1)(ii)(B)	Security Management Process -- Risk Management	§164.308(a)(1)(ii)(B): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	Does the entity have policies and procedures in place regarding a risk management process sufficient to r reasonable and appropriate level? Has the entity implemented security measures sufficient to reduce risks and vulnerabilities to a reasonabl Obtain and review policies and procedure related to risk management. Evaluate and determine if the docu what is considered an acceptable level of risk based on management approval, the frequency of reviewing members' roles in the risk management process. Obtain and review documentation demonstrating the security measures implemented and/or in the proces
Security	§164.308(a)(1)(ii)(C)	Security Management Process – Sanction Policy	§164.308(a)(1)(ii)(C): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	Does the entity have policies and procedures in place regarding sanctions to apply to workforce members security policies and procedures? Does the entity apply appropriate sanctions against workforce members who fail to comply with its securi Obtain and review documentation of the sanction policies and procedures (which could be an aspect of a contain a reasonable and appropriate process to sanction workforce members for failures to comply with t

U.S. Dept of Health and Human Services. Retrieved from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/

What Should You Do?

1. Protect Information
2. Meet Regulations



Am I Too Small?

Dermatology practice settles potential HIPAA violations

Adult & Pediatric Dermatology, P.C., of Concord, Mass., (APDerm) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules with the Department of Health and Human Services, agreeing to a $150,000 payment. APDerm will also be required to implement a corrective action plan to correct deficiencies in its HIPAA compliance program. APDerm is a private practice that delivers dermatology services in four locations in Massachusetts and two in New Hampshire. This case marks the first settlement with a covered entity for not having policies and procedures in place to address the breach notification provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA).

The HHS Office for Civil Rights (OCR) opened an investigation of APDerm upon receiving a report that an unencrypted thumb drive containing the electronic protected health information (ePHI) of approximately 2,200 individuals was stolen from a vehicle of one its staff members. The thumb drive was never recovered. The investigation revealed that APDerm had not conducted an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality of ePHI as part of its security management process. Further, APDerm did not fully comply with requirements of the Breach Notification Rule to have in place written policies and procedures and train workforce members.

"As we say in health care, an ounce of prevention is worth a pound of cure," said OCR Director Leon Rodriguez. "That is what a good risk management process is all about – **identifying and mitigating the risk before a bad thing happens. Covered entities of all sizes need to give priority to securing electronic** protected health information."

In addition to a $150,000 resolution amount, the settlement includes a corrective action plan requiring AP Derm to develop a risk analysis and risk management plan to address and mitigate any security risks and vulnerabilities, as well as to provide an implementation report to OCR.

US Department of Health and Human Services. Dermatology practice settles potential HIPAA violations,, December 26, 2013

Am I Too Small?

Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to $650,000 HIPAA Settlement

Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule after the theft of a CHCS mobile device compromised the protected health information (PHI) of hundreds of nursing home residents. CHCS provided management and information technology services as a business associate to six skilled nursing facilities. The total number of individuals affected by the combined breaches was 412. The settlement includes a monetary payment of $650,000 and a corrective action plan.

…..

OCR initiated its investigation on April 17, 2014, after receiving notification that CHCS had experienced a breach of PHI involving the theft of a CHCS-issued employee iPhone. The iPhone was unencrypted and was not password protected. The information on the iPhone was extensive, and included social security numbers, information regarding diagnosis and treatment, medical procedures, names of family members and legal guardians, and medication information. At the time of the incident, CHCS had no policies addressing the removal of mobile devices containing PHI from its facility or what to do in the event of a security incident; OCR also determined that CHCS had no risk analysis or risk management plan.

US Department of Health and Human Services. Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to $650,000 HIPAA Settlement,, July 3, 2016

Am I Too Small?

HHS announces first HIPAA breach settlement involving less than 500 patients

Hospice of North Idaho settles HIPAA security case for $50,000

The Hospice of North Idaho (HONI) has agreed to pay the U.S. Department of Health and Human Services' (HHS) **$50,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. This is the first settlement involving a breach of unsecured electronic protected health information (ePHI) affecting fewer than 500 individuals.**

The HHS Office for Civil Rights (OCR) began its investigation after HONI reported to HHS that an unencrypted laptop computer containing the electronic protected health information (ePHI) of 441 patients had been stolen in June 2010. Laptops containing ePHI are regularly used by the organization as part of their field work. Over the course of the investigation, OCR discovered that HONI had not conducted a risk analysis to safeguard ePHI. Further, HONI did not have in place policies or procedures to address mobile device security as required by the HIPAA Security Rule. Since the June 2010 theft, HONI has taken extensive additional steps to improve their HIPAA Privacy and Security compliance program.

"This action sends a **strong message to the health care industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their** patients' health information." said OCR Director Leon Rodriguez. "Encryption is an easy method for making lost information unusable, unreadable and undecipherable."

US Department of Health and Human Services. HHS announces first HIPAA breach settlement involving less than 500 patients,, January 2, 2013

Am I Too Small?

HIPAA Settlement Highlights the Continuing Importance of Secure Disposal of Paper Medical Records

(now out of business)

Cornell Prescription Pharmacy (Cornell) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule with the Department of Health and Human Services (HHS), Office for Civil Rights (OCR). Cornell will pay $125,000 and adopt a corrective action plan to correct deficiencies in its HIPAA compliance program. Cornell is a small, single-location pharmacy that provides in-store and prescription services to patients in the Denver, Colorado metropolitan area, specializing in compounded medications and services for hospice care agencies in the area.

OCR opened a compliance review and investigation after receiving notification from a local Denver news outlet regarding the disposal of unsecured documents containing the protected health information (PHI) of 1,610 patients in an unlocked, open container on Cornell's premises**. The documents were not shredded and contained identifiable information regarding specific patients. Evidence obtained by OCR during its investigation revealed** Cornell's **failure to implement any written policies and procedures as required by the HIPAA Privacy Rule. Cornell also failed to provide training on policies and procedures to its workforce as required by the Privacy Rule.**

"**Regardless of size, organizations cannot abandon protected health information or dispose of it in dumpsters or** other containers that are accessible by the public or other unauthorized persons," said OCR Director Jocelyn Samuels. "Even in our increasingly electronic world, it is critical that policies and procedures be in place for secure **disposal of patient information, whether that information is in electronic form or on paper**

US Department of Health and Human Services. HIPAA Settlement Highlights the Continuing Importance of Secure Disposal of Paper Medical Records, Apr 22, 2015

Cyber Risk

1. Downtime/Business Disruption
2. Office for Civil Rights HIPAA Violation (Breach)
    1. Investigation
    2. Fines/Penalties
    3. Corrective Action Plan
3. Civil Litigation
4. Reputation Damage
5. Individual Notification/Credit Monitoring Costs
6. Legal Expenses
7. Forensic/Repair

Cyber Attack Techniques

Motivators

1. Money
2. Fun
3. Social/Political Cause
4. Information

Best Practice Stages

1. Reconnaissance
2. Scan
3. Gain Access
4. Maintain Access
5. Clear Tracks

Attack Stages - Analogy

Stage	Burglar - Your House	Hacker - Your Organization
Reconnaissance	• Drive by - schedule • Look at county auditor site • Facebook	• LinkedIn • Google • SEC Filings • Website
Scanning	• Check doors, windows • Try garage codes	• Scan ports • Phone calls • Physical visit
Gain Access	• Enter through window	• Phishing • Malware • Social
Maintain Access	• Add garage code • Find spare key	• Create back door • Create user
Clear Tracks	• Leave house as was • Remove fingerprints	• Clear audit logs

Access Methods - Social Engineering

Phishing

Spear Phishing

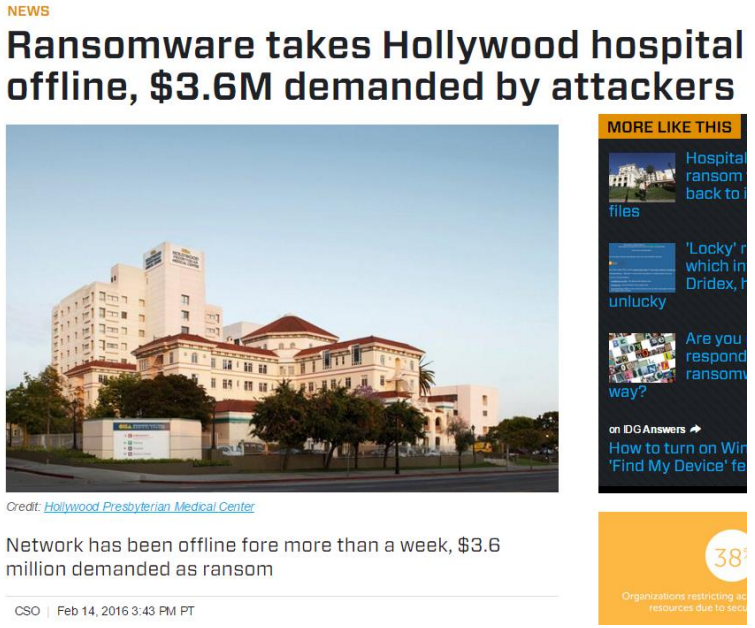
Whaling

Ransomware

- Malware
- Enters through infected Ads or files
- Encrypts files
- Ransom demanded for key
- Usually no data is stolen

Countermeasures

- Security Awareness Training
- Off-line and regular backups
- Lowest system privileges
- System/Antivirus Updates


NEWS

Ransomware takes Hollywood hospital offline, $3.6M demanded by attackers

Credit: Hollywood Presbyterian Medical Center

Network has been offline fore more than a week, $3.6 million demanded as ransom

CSO | Feb 14, 2016 3:43 PM PT

MORE LIKE THIS

Hospital ransom back to files

'Locky' which in Dridex, unlucky

Are you respond ransom way?

on IDG Answers

How to turn on Wi 'Find My Device' fe

38

Organizations restricting ac resources due to secu

CSO,February, 14, 2016
http://www.csoonline.com/article/3033160/security/ransomware-takes-hollywood-hospital-offline-36m-demanded-by-attackers.html

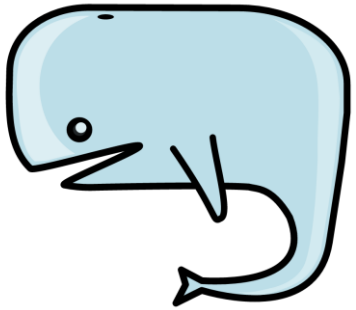
HIMSS CENTRAL & SOUTHERN OHIO Chapter

WannaCry?

- Ransomware
- Entered through phishing emails or infected websites
- Ransom demanded for key
- Exploits unpatched Windows devices

Each infection demands a $300 bitcoin payment to unlock that computer's files, leading to massive downtime while breached companies attempt to make payments and wait for unlock keys to come back from the cybercriminals.

Whaling



- Targets high-profile end users (C-Level)
- Usually through email
- Have familiarity with your company
- Sense of urgency to wire money

Countermeasures

- Security Awareness Training
- Follow Policies and Procedures

Technology

'Whale' finance fraud hits businesses

19 October 2015 | Technology

Fraudsters have wrung millions out of victims of "whaling" fraud

Cyber-thieves are stealing millions of pounds, with a scam based around faking email messages from company bosses.

Source: BBC

Technical Attack Details

- Gain access to network or device on network
  - Phish
  - Wireless
  - Web-facing application
  - Etc.
- Passively listen to traffic
- Pivot
  - Steal Passwords – electronically or phish
  - Look for other vulnerabilities
  - Gain access to file shares, EHR, etc.
  - Gain Domain Admin password

Blue Orange Penetration Test Stats

- 15-25%
  - When phishing for credentials we typically see 15-25% of our targets provide credentials.
- 15-20 minutes
  - Passwords electronically cracked
- 3 hours
  - After gaining an initial account it usually takes ~3 hours to attain domain admin.
- 30-60 minutes
  - With domain admin it is usually instant or takes another ~30-60 minutes to gain EMR access.

Blue Orange Real-World Example

Example 1

1. Cracked pwd electronically
2. Found workstation using pwd ad local admin
3. Found file with all uname/pwd pairs

Example 2

1. Gained access to multiple accounts via phishing
2. Found published script on their domain controller that included their local administrator credentials
3. Used compromised local administrator credentials to harvest domain administrator credentials

Cyber Security Vulnerabilities

Technical

- Software Patches
- Open Ports
- Wireless
- Anti-virus/malware
- Weak passwords
- Unmanaged accounts
- Encryption
- Non-secure web-facing application
- Default accounts
- Mobile devices

Human

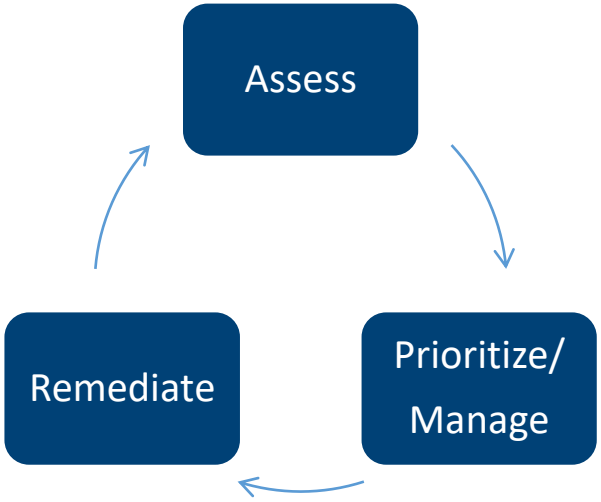
- Password sharing
- Phone skills
- Links

Physical

- Wired ports
- Visitor management

Prevention - Security

- Assess
  - Perform **thorough and accurate** Risk Analysis
  - Develop and **actively manage** security plan
  - Remediate
  - Rinse and repeat
- Test
  - Vulnerability Scans - External/Internal
  - Penetration Test
- Train
  - Workforce
  - IT Specific



- Include in Risk Management
  - Include in Executive Meeting Agenda
  - Share with Board of Directors
  - This is NOT just an “I.T. Thing”

Prevention

- Vulnerability Scan
  - Internal
  - External
- Penetration Test
  - White Box
  - Black Box

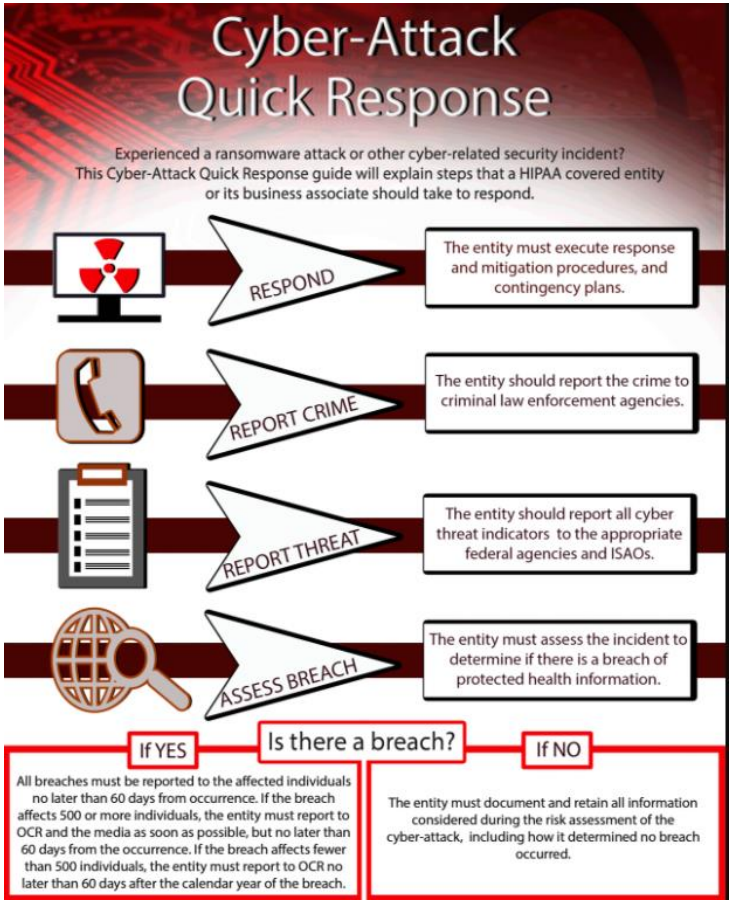
Preparation/Response

- “It’s not if, it’s when”

- HIPAA Regulatory Conformance
- Incident response Plan
- Breach Response
- Cyber Insurance

Office for Civil Rights (OCR) Quick Response Guidance

- Respond and Mitigate
- Report Crime
- Report Threat
- Assess Breach (Risk Assessment)
- If Breach
  - Report as required per HIPAA Breach Regulations
- Else
  - Document Risk Assessment



Cyber Insurance

Information Security Policies

1. Has the **Applicant** implemented a formal information security policy which is applicable to a the **Applicant's** business units?

   If "Yes",

   (a) Does the **Applicant** test the security required by the security policy at least annually?

   (b) Does the **Applicant** regularly identify and assess new threats and adjust the security p to address the new threats?

   (c) Does the **Applicant's** information security policy include policies for the use and storag personally identifiable or other confidential information on laptops?

Web Server Security

1. Does the **Applicant** store personally identifiable or other confidential information on their servers?
2. Do the **Applicant's** web servers have direct access to personally identifiable or other confide information?
3. Does the **Applicant** have firewalls that filter both inbound and outbound traffic?

Virus Prevention, Intrusion Detection & Penetration Testing

1. Are anti-virus programs installed on all of the **Applicant's** PC's and network systems?

   If "Yes", how frequently are the virus detection signatures updated?

2. Does the **Applicant** employ intrusion detection or intrusion protection devices on their netw or IDS or IPS software on the **Applicant's** hosts?

   If "Yes", how frequently are logs reviewed? _____

3. Does the **Applicant** run penetration tests against all parts of their network?

   If "Yes", how often are the tests run? _____

4. Has the **Applicant** been the target of any computer or network attacks (including virus attack the past 2 years?

   If "Yes", did the number of attacks increase?

Mobile Device Security

1. Does the **Applicant** store personally identifiable or other confidential information on mo devices?

   If "Yes", does the **Applicant** encrypt such information?

Business Continuity

1. Does the **Applicant** have a Business Continuity Plan [BCP] specifically designed to address a network related denial-of-service attack? ☐ Yes ☐ No

Security Assessments

1. Has an external system security assessment, other than vulnerability scans or penetration tests, been conducted within the past 12 months? ☐ Yes ☐ No

   If "Yes", please indicate who conducted the assessment, attach copies of the result, and indicate whether all critical recommendations been corrected or complied with.

   If "No", please attach explanation.

Backup & Archiving

1. How frequently does the **Applicant** back up electronic data? _____
2. Does the **Applicant** store back up electronic data with a third party service provider? ☐ Yes ☐ No

   (a) If "Yes", does the **Applicant** have a written contract with the respective service provider(s)? ☐ Yes ☐ No

   (b) If "Yes" to 2(a), does the **Applicant's** contract with the service provider(s) state that the service provider:

   i) Has primary responsibility for the security of the **Applicant's** information? ☐ Yes ☐ No

   ii) Have a contractual responsibility for any losses or expenses associated with any failure to safeguard the **Applicant's** electronic data? ☐ Yes ☐ No

   iii) Does the **Applicant** review their most recent information security audit (i.e. SAS 70)? ☐ Yes ☐ No

Service Providers

1. Does the **Applicant** use third-party technology service providers? ☐ Yes ☐ No

   (a) If "Yes", does the **Applicant** have a written contract with the respective service provider(s)? ☐ Yes ☐ No

   (b) If "Yes" to 1(a), does the **Applicant's** contract with the service provider(s) state that the service provider:

   i) Has primary responsibility for the security of the **Applicant's** information? ☐ Yes ☐ No

   ii) Have a contractual responsibility for any losses or expenses associated with any failure to safeguard the **Applicant's** electronic data? ☐ Yes ☐ No

   iii) Does the **Applicant** review their most recent information security audit (i.e. SAS 70)? ☐ Yes ☐ No

Incident Response Plans

1. Does the **Applicant** have a formal incident response plan that addresses network security incidents or threats? ☐ Yes ☐ No

HIMSS CENTRAL & SOUTHERN OHIO Chapter

Governance

- HIPAA Security Officer
- HIPAA Privacy Officer
- Compliance Committee
- Executive Oversight
- Board Communication
- Cyber Insurance Carrier

Additional Information

Download OCR Audit E Book

www.blueorangecompliance.com

Download Cyber Security E Book

www.blueorangecompliance.com

OCR Cyber Guidance

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

OCR Audit Protocol

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html

HHS Breach "Wall of Shame"

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

HIMSS CENTRAL & SOUTHERN OHIO Chapter

Organization Questions

- Have you performed a HIPAA security risk analysis? Has it been regularly updated?
- Do you have an active security plan?
- Do you have operational policies and procedures for Security? Privacy? Breach?
- Have they been updated since Omnibus (2013)?
- Has your staff been trained in HIPAA and your policies and procedures?
- Do you have a HIPAA Privacy officer and Security Officer designated?
- Have you reviewed the latest Office for Civil Rights HIPAA Audit protocol?

Thank You

Contact Info and Additional Information

John DiMaggio, CEO
Blue Orange Compliance
John.dimaggio@blueorangecompliance.com
614.567.4109

BLUE ORANGE COMPLIANCE

HIMSS CENTRAL & SOUTHERN OHIO Chapter