# Security in a HealthCare – What you need to know

Lunch and Learn Webinar
August 10, 2016

HIMSS
CENTRAL & SOUTHERN OHIO *Chapter*

# About the Presenter

*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 and healthcare associations including HIMSS, 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.

*John DiMaggio, CEO*
*Blue Orange Compliance*
*5131 Post Rd*
*Dublin, OH 43017*
*john.dimaggio@blueorangecompliance.com*
*614.270.9623*

# About Blue Orange

National Provider

Specialize in healthcare information privacy and security solutions.

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.

- HIPAA Security Risk Analyses & Remediation
- HIPAA Privacy and Breach Assessments & Remediation
- Penetration Testing
- Forensics
- Mock Office for Civil Rights HIPAA Audits

BLUE ORANGE® COMPLIANCE

HIMSS CENTRAL & SOUTHERN OHIO *Chapter*

# Agenda

- Privacy and Security in Perspective
- Laws and Regulations
- Office for Civil Rights New Audit Protocol
- Cyber Security in the News
- Mitigation
- Call to Action

# 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?

# Healthcare Landscape

## Healthcare

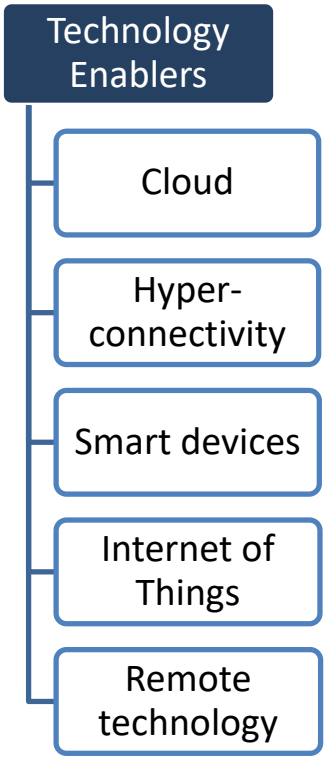
- Electronic
- Push toward interoperability
- Cost shift outside 4 walls
- Information outside 4 walls

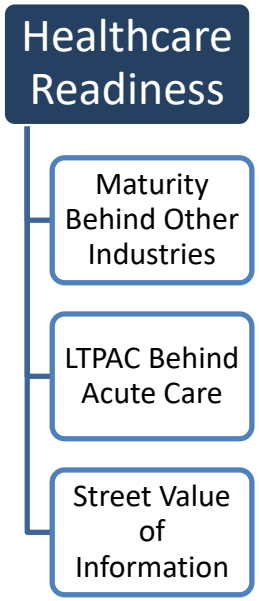
## Acute Care

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

## LTPAC

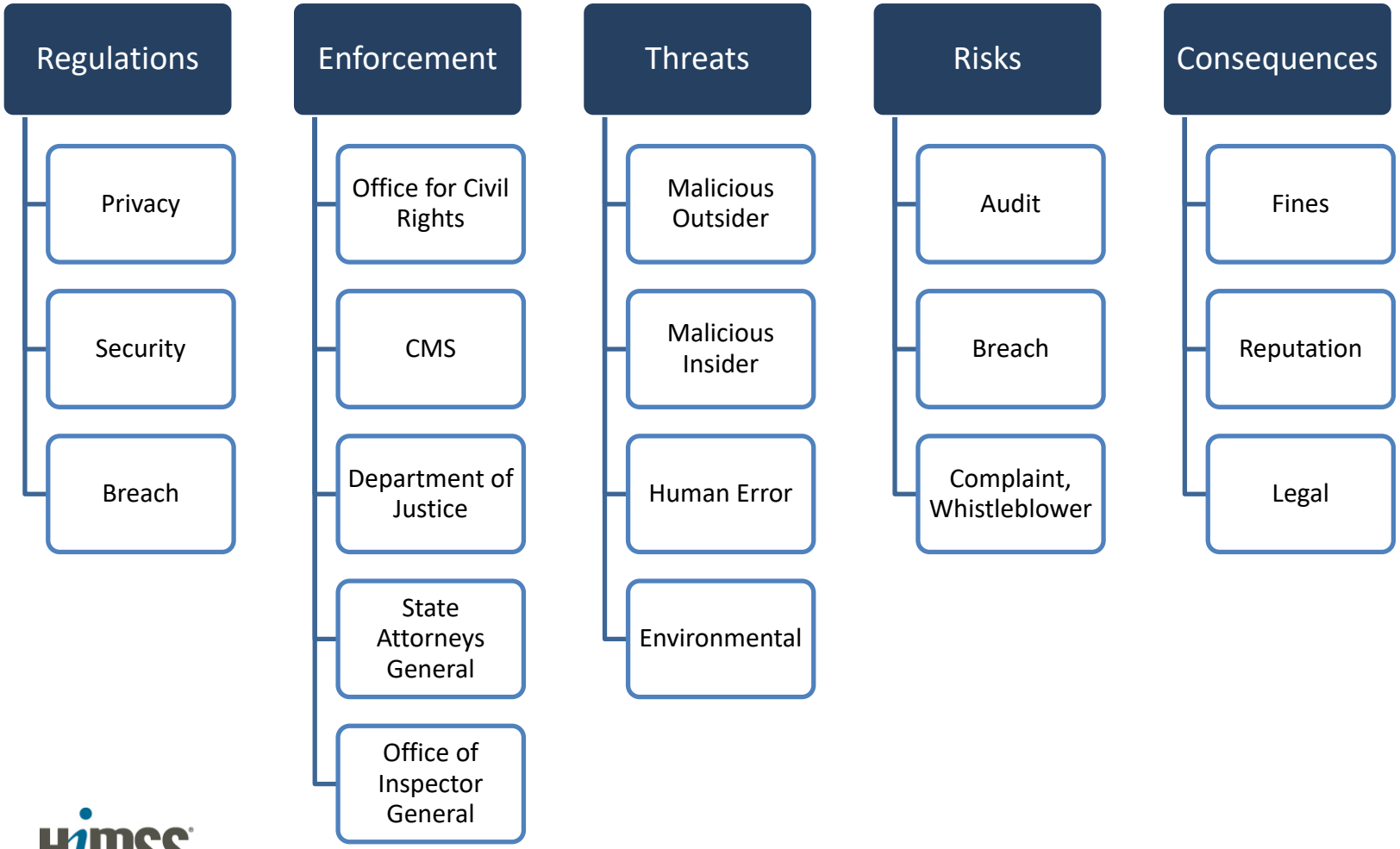
- Push toward interoperability
- Implementing EHR
- Implementing applicable technology




HIMSS CENTRAL & SOUTHERN OHIO *Chapter*

# Privacy and Security



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.

# Is Privacy and Security  Important?

- Who thinks it is important?
- Government
- Clients (Business Associate)
- Insurance Companies
- Your patients and residents

- What will happen if we don't manage it?
- It's not "if", it's "when"
- Random Audit
- For Cause Audit
- Breach
- Legal
- Reputation

# 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.

# 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."

# Am I Too Small?

## Bad News for HIPAA Business Associates: HHS OCR Announces $650,000 Settlement for BA Breach

Posted on July 3rd, 2016 by Colin Zick

Catholic Health Care Services of the Archdiocese of Philadelphia ("CHCS"), a HIPAA business associate, has agreed to pay the Department of Health and Human Services Office of Civil Rights ("OCR") $650,000 in connection with a data breach involving the nursing homes to which it provides management and IT services.

The underlying breach occurred in February 2014 (which suggests a significant backlog at OCR in resolving open matters). The breach itself was relatively insignificant compared to those we often see today involving millions of records: this was the theft of an unsecured iPhone with health information of 412 nursing home patients.

The resolution agreement's formal description of the problematic behavior was: "From September 23, 2013, the compliance date of the Security Rule for business associates, until the present, CHCS failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality integrity, and availability of e-PHI held by CHCS." The specifics, according to OCR's statement about the settlement, are as follows:

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.

In determining the resolution amount, OCR considered that CHCS provides unique and much-needed services in the Philadelphia region to the elderly, developmentally disabled individuals, young adults aging out of foster care, and individuals living with HIV/AIDS.

Given that CHCH is 1) a non-profit; 2) with a religious affiliation; 3) providing "much-needed services"; and 4) "only" 412 records were involved, the $650,000 settlement and two-year corrective plan is significant and sends a clear message: business associates that are involved in breaches are going to be treated just as if they are covered entities by OCR when it comes to resolution of breaches

# 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.

# Why HIPAA?

- *Exchange and transmit claims information in a standard way*

- *Public feel safe their health information is protected*
  - *How information can be shared*
  - *Patient rights*
  - *Specifics around protecting electronic 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)

# What's at Risk? Penalties Plus…

## *Civil Monetary Penalties*

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

## Other Costs

- Legal
- Accelerated Remediation
- Public Relations
- Reputation


HIMSS CENTRAL & SOUTHERN OHIO *Chapter*

Cleanup from a HIPAA Breach can cost an organization:

A) $58,000
B) $830,000
C) $2,400,000
D) Nothing.  It's no big deal.

# 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*

# Privacy, Security, Breach Scope

Security

- "C.I.A." Confidentiality, Integrity, Availability
- HIPAA Security Rule Safeguards
  - Administrative
  - Technical
  - Physical
  - Organizational

Privacy

Patient Rights
Uses and Disclosures
Training
Business Associates
Forms, logs, reports, audit

Breach

Detection
Mitigation
Documentation
Notification
Training

*Example Security Control Families*

*Access Control*
*Audit and Accountability*
*Certification, Accreditation, and Security Assessment*
*Configuration Management*
*Contingency Planning*
*Identification and Authentication*
*Incident Response*
*Maintenance*
*Media Protection*
*Physical and Environmental*
*Security Planning*
*Security Awareness and Training*
*Personnel Security*
*Risk Assessment*
*System and Service Acquisition*
*System and Communications*
*System and Information Integrity*

# 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*

# Office for Civil Rights HIPAA Audits

- Random Audits
  - Performed Test Audits in 2012
  - 2016 Audits Underway
  - New Audit Protocol Published April, 2016

- For Cause Audits/Investigations
  - Incident or Breach
  - Whistleblower
  - Complaint

# OCR HIPAA Audits

- 2016 in process
- Covered Entities and Business Associates
- Email verification
- Questionnaire
- Audit pool selection
- Desk Audits  - Have 10 days to send requested information

**Subject: Audit Entity Contact Verification**

DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE OF THE SECRETARY

Voice - (800) 368-1019
TDD - (202) 619-2357
FAX - (202) 619-3818
http://www.hhs.gov/ocr

Director
Office for Civil Rights
200 Independence Ave., SW; RM 509F
Washington, DC 20201

05/20/2016

You
Your Location
Your Address
Your City, State, ZIP

Dear Contact:

This is an automated communication from the Office for Civil Rights (OCR).

According to our records, you are the primary contact OCR should use to reach YOUR COVERED ENTITY regarding its potential inclusion in the HIPAA Privacy, Security, and Breach Notification Rules Audit Program. We are attempting to verify this email address.

Please respond within fourteen (14) days as instructed below to either confirm your identity and email address or instead provide updated primary and secondary contact information.

If you ARE the primary contact for this organization, please select the following link YES. Once the link is selected, a browser window will open and your response will be recorded.

If you ARE NOT the primary contact for this organization, please select the following link NO. Once the link is selected, a browser window will open and your response will be recorded.

Thank you for your cooperation. If we do not receive a response from you we will use this email address for future communications with this entity. Failure to respond will not shield your organization from selection.

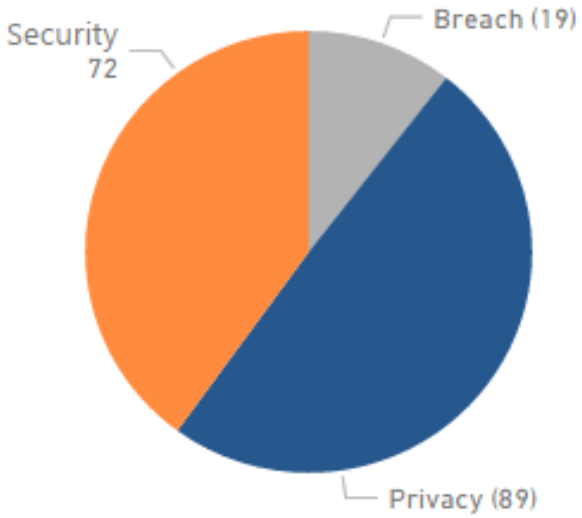
If you have questions or comments regarding this message, you may contact us at OSOCRAudit@hhs.gov.

Sincerely,

Jocelyn Samuels
Director
Office for Civil Rights
OFFICE OF THE SECRETARY
Department of Health and Human Services
http://www.hhs.gov/ocr

# 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 if 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<br><br>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?<br><br>Determine how the entity has implemented the requirements.<br><br>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.<br><br>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:<br>• A defined scope that identifies all of its systems that create, transmit, maintain, or transmit ePHI<br>• Details of identified threats and vulnerabilities<br>• Assessment of current security measures<br>• Impact and likelihood analysis<br>• Risk rating<br><br>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?<br><br>Has the entity implemented security measures sufficient to reduce risks and vulnerabilities to a reasonabl<br><br>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.<br><br>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?<br><br>Does the entity apply appropriate sanctions against workforce members who fail to comply with its securi<br><br>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 |

# OCR Audit Protocol Walkthrough
# Privacy Example

| # | Audit Type | Section | Key Activity | Established Performance Criteria | Audit Inquiry |
|---|---|---|---|---|---|
| 12 | Privacy | §164.506(b); (b)(1); and (b)(2) | Consent for uses and disclosures | §164.506(b) - Standard: Consent for uses and disclosures permitted.<br><br>§164.506(b)(1) A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations. | Does the entity obtain the individual's consent for uses and disclosures?<br><br>Obtain samples of completed consents, if any, and patient intake materials and review to determine if its u performance criterion. |
| 13 | Privacy | §164.508(a)(1-3) and §164.508(b)(1-2) | Authorizations for uses and disclosures is required | §164.508(a)(1) Authorization required: General rule.<br>Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.<br><br>§164.508(a)(2) Authorization required: Psychotherapy notes.<br>(i) Notwithstanding any provision of this subpart, other than the transition provisions in §164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:<br>(i) To carry out the following treatment, payment, or health care operations:<br>(A) Use by the originator of the psychotherapy notes for treatment;<br>(B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or<br>(C) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and<br>(ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).<br><br>§164.508(a)(3) Authorization required: Marketing.<br>(i)Notwithstanding any provision of this subpart, other than the transition provisions in §164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the | What policies and procedures exist for obtaining a valid authorization when required?<br>Do policies and procedures exist to determine when authorization is required?<br><br>Obtain and review against the established performance criterion the policies and procedures for obtaining standard:<br>-Documentation of covered entity policy and procedures<br>-Documentation that a standard covered entity authorization, if any, is valid<br><br>Obtain and evaluate a sample of authorizations obtained to permit disclosures for consistency with the es entity-established policies and procedures.<br>For providers only: obtain and review all relevant patient intake forms for both inpatient and outpatient ser authorization forms, if any, to assess whether the provider's practice is to use a consent when an authoriz disclosure of information pursuant to the consent. |
| 14 | Privacy | §164.508(b)(3) | Compound authorizations | §164.508(b)(3) Compound authorizations. An authorization for use or disclosure of protected health information may not be | Does the covered entity use or disclose PHI for the purpose of research, conducts research, provides psy compound authorizations? |

# OCR Audit Protocol Walkthrough

## Breach Example

| # | Audit Type | Section | Key Activity | Established Performance Criteria | Audit Inquiry |
|---|---|---|---|---|---|
| 162 | Breach | §164.414(a) | Administrative Requirements | §164.414(a) Administrative Requirements. A covered entity is required to comply with the administrative requirements of §164.530(b), (d), (e), (g), (h), (i), and (j) with respect to 45 CFR Part 164, Subpart D ("the Breach Notification Rule"). | 164.414(a) Administrative Requirements: Has the covered entity adequately implemented the required 164.530 provis Notification Rule? Inquire of management. |
| 163 | Breach | §164.530(b) | Training | §164.530(b) Training. All workforce members must receive training pertaining to the Breach Notification Rule. | 164.530(b) - Training Obtain and review the covered entity's policies and procedures. Evaluate whether they are consistent wit pertaining to the Breach Notification Rule.<br><br>Has the covered entity trained its workforce on the applicable provisions?<br>• Obtain and review the content of covered entity's training materials |
| 164 | Breach | §164.530(d) | Complaints | 164.530(d) Complaints. All covered entities must provide a process for individuals to complain about its compliance with the Breach Notification Rule. | 164.530(d) - Complaints to the covered entity Obtain and review the covered entity's policies and procedures. Evaluate whether they are consistent wit for individuals to complain about the covered entity's compliance with the Breach Notification Rule.<br><br>Does the covered entity have a process in place for individuals to complain about its compliance with the<br>Has the covered entity received any such complaints? If yes, obtain and review a list of complaints recei |
| 165 | Breach | §164.530(e) | Sanctions | 164.530(e) Sanctions. All covered entities must sanction workforce members for failing to comply with the Breach Notification Rule. | 164.530(e) – Sanctions Obtain and review the covered entity's policies and procedures. Evaluate whether they are consistent wit entity's workforce members.<br><br>Has the covered entity sanctioned any workforce members for failing to comply with its policies and proce Notification Rule? If yes, obtain and review a complete list of sanctions, including the type of sanction app sanction and any other relevant information. Use sampling methodologies to select sanctions to be review |
| 166 | Breach | §164.530(g) | Refraining from Retaliatory Acts | 164.530(g) Refraining from Retaliatory Acts. All covered entities must have policies and procedures in place to prohibit retaliatory acts. | 164.530(g) – Refraining from Retaliatory Acts Does the covered entity have appropriate policies and procedures in place to prohibit retaliation against a participating in a process (e.g., assisting in an investigation by HHS or other appropriate authority or for fil or practice that the person believes in good faith violates the Breach Notification Rule? Obtain and review |
| 167 | Breach | §164.530(h) | Waiver of Rights | 164.530(h) Waiver of Rights. All covered entities must have policies and procedures in | 164.530(h) – Waiver of Rights Does the covered entity have appropriate policies and procedures in place to prohibit it from requiring an Breach Notification Rule as a condition of the provision of treatment, payment, enrollment in a health plan, |
| 168 | Breach | §164.530(i) | Policies and Procedures | 164.530(i) Policies and Procedures. All covered entities must have policies and procedures that are consistent with the requirements of the Breach Notification Rule. | 164.530(i) – Policies and Procedures Does the covered entity have policies and procedures that are consistent with the requirements of the Br<br>• Obtain and review the covered entity's policies and procedure for evaluating the appropriate action unde there is an impermissible use or disclosure of PHI.<br>• Obtain and review the covered entity's policies and procedures for providing notifications to individuals, Secretary.<br>• Obtain and review the covered entity's policies and procedures for requiring business associates to rep |

# OCR Audit Protocol Additional Information

Download OCR Audit E Book

www.blueorangecompliance.com

Audit Protocol

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

HIMSS CENTRAL & SOUTHERN OHIO Chapter

# Governance

- HIPAA Security Officer
- HIPAA Privacy Officer
- Executive Oversight
- Board Communication

# HIPAA Security Risk Analysis

- Required by HIPAA Regulations
- Thorough and Accurate – Assess all required areas
- Perform Regularly

# Considerations

- Policies/procedures alone are not enough – they need to be communicated and understood
- Your weakest link is the employee you hired yesterday – training is not a “one-time-only” deal
- Business Associate Agreements and Confidentiality Statements are not enough. What happens when the ink dries? Are the contractual terms communicated to those with day-to-day responsibility?
- Compliance must be monitored and consistently enforced

# Cyber Security

## Hacking Stages

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

## Hacking Motivators

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

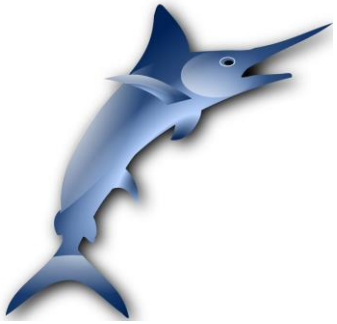
# Hacking Stages

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

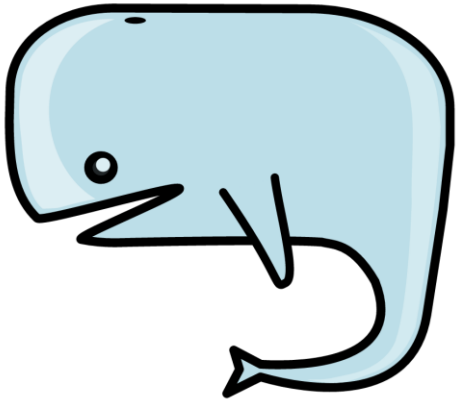
# Social Engineering

Phishing

Spear Phishing



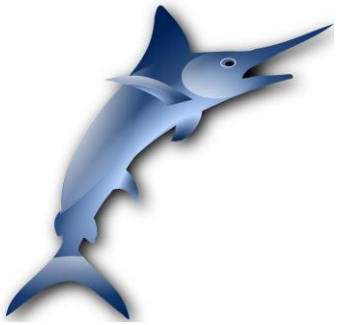
Whaling



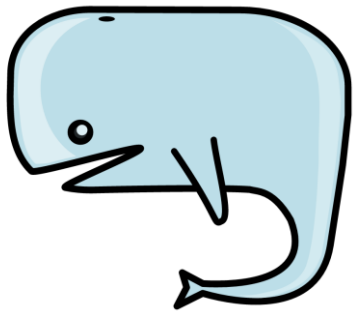
# Phishing and Spear Phishing

Phishing
- Email-based
- Broad Targets
- Offer something of value

Spear Phishing
- Email-based
- Selected Targets
- Custom, Legitimate-looking Message



# 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

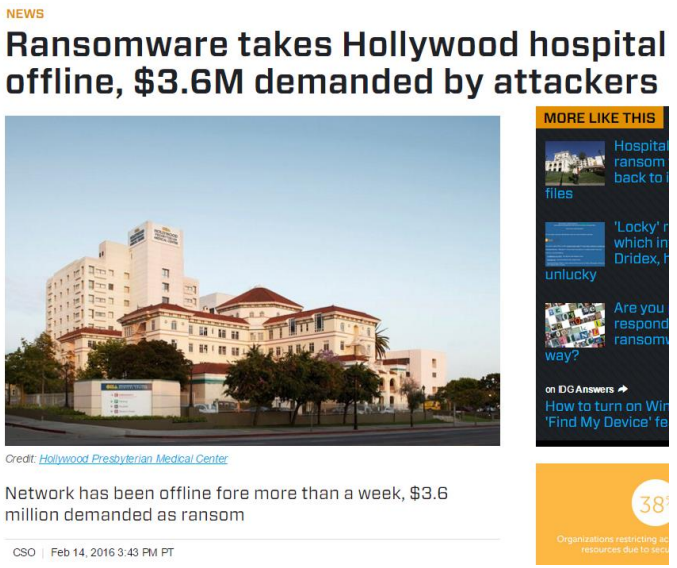

Fraudsters have wrung millions out of victims of "whaling" fraud

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

Source: BBC

# Ransomware

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




Source: CSO

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

Post Incident
- Incident Response
- Breach Policies and Procedures

HHS Guidance:
https://www.hhs.gov/blog/2016/07/11/your-money-or-your-phi.html

HIMSS CENTRAL & SOUTHERN OHIO Chapter

# Security Mitigation

- Risk Analysis
- Vulnerability Scanning
  - External
  - Internal
  - Web Application Testing
- Penetration Test
- Policies and Procedures
- Security Awareness Training and Regular Alerts

# Passwords

- Last Line of Defense

- Password Cracking
  - Non-Electronic
    - Shoulder Surfing
    - Dumpster Diving
    - Social Engineering
  - Electronic
    - Guessing
    - Default Passwords
    - Electronic Cracking

# Passwords - Mitigation

- Password length and complexity
- Failed login attempts
- Regular forced password changes
- De-activate account if not used in x days
- 2-factor authentication if possible

# Encryption

- Scrambling Information with a Key
- In transit
- At Rest

# Cyber Security Additional Information

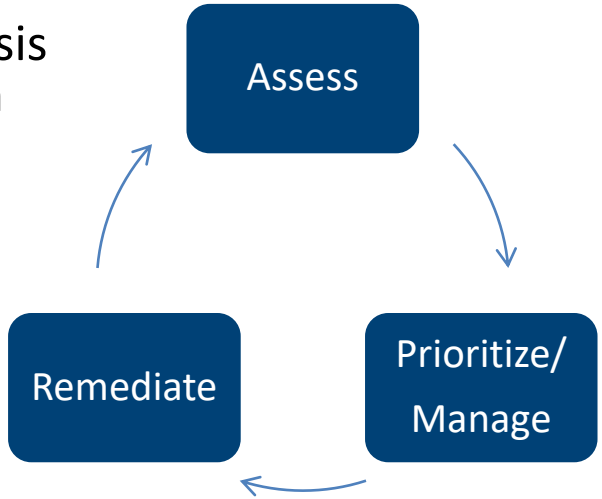
Download Cyber Security EBook
www.blueorangecompliance.com

# Physical Security

- Locked doors
- Visitor Management
- Training

# Call to Action - Security

- Assess
  - Perform **thorough and accurate** Risk Analysis
  - Develop and **actively manage** security plan
  - Remediate
  - Rinse and repeat
- Test
  - Vulnerability Scans - External/Internal
  - Web Application Testing
  - 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”

# Call to Action – Privacy and Breach

- Perform Gap Analysis
  - Evaluate Policies and Procedures
  - Review HIPAA Entity Designation
  - Review Business Line Regulations
  - Review State Regulations
  - Review Operations

# 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*
*614.270.9623*

BLUE ORANGE® COMPLIANCE

HIMSS CENTRAL & SOUTHERN OHIO *Chapter*