HIPAA/HITECH Privacy and Security for Long Term Care
John DiMaggio
• Chief Executive Officer, Blue Orange Compliance

Cliff Mull
• Partner, Benesch, Healthcare Practice
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, and long term care associations including LTPAC, NAHC and ALFA. John is also a LeadingAge CAST Commissioner.

John’s extensive long term and post-acute care 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.

**W. Cliff Mull, Partner, Benesch, Healthcare Practice**

Mr. Mull is a Partner in the firm’s Health Care Practice Group. Mr. Mull’s practice focuses on advising physicians and health care, life sciences, pharmaceutical and device businesses on regulatory, business and intellectual property issues. He has represented physicians, limited licensed practitioners, physician and multi-specialty group practices, ambulatory surgery centers, durable medical equipment suppliers, medical device manufacturers and distributors, hospice agencies, pharmacies and other ancillary service providers.

Mr. Mull regularly counsels clients on a number of regulatory issues, including licensure, certification and accreditation; HIPAA and state privacy laws, and state and federal fraud abuse laws, including the state and federal anti-kickback statutes, the Stark Physician Self Referral Law and the False Claims Act. Mr. Mull also counsels clients in the healthcare industry and other industries with respect to business transactions and general business counseling, including formation, reorganization, mergers and acquisitions, and joint ventures; corporate governance; negotiation and drafting of contracts, including employment agreements, consulting agreements, service agreements, supply and distribution agreements.
Topics

- Privacy and Security Regulation Overview
- OCR Audit Protocol
- Other Enforcement
- Interoperability
- Acute Care I.T. Priorities
- Assessment Data
- Cloud
- Cyber Insurance
- Governance
HIPAA Background

- What is HIPAA? Health Insurance Portability and Accountability Act
- Why HIPAA?
- Timeline
  - 2003 HIPAA Privacy
    - HIPAA Became Law
    - Scope & Enforcement
  - 2005 Added Security Rule
    - Scope
    - Enforcement
  - 2010 HITECH
    - Added scope
    - Increased enforcement & penalties
  - 2012 OCR HIPAA “Test Audits”
  - 2013 Omnibus
    - Rule modifications
  - 2015 OCR Audits Resume
**HIPAA and HITECH**

**HITECH Goals**
- Government Involvement for Adoption
- Financial Incentives for Adoption
- Savings
- **Strengthen Privacy & Security Laws**

Increased HIPAA Scope after HITECH
- Business Associates
- Breach Reporting
- Enforcement
- Civil & Criminal Penalties
- Privacy
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 inquiries, 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.
Enforcement

Government Enforcement

• Office for Civil Rights
• CMS
• State Attorneys General
• Department of Justice

Consequences

• Fines and Penalties
• Legal Costs
• Government Corrective Action Plan
• Reputation
• Civil Actions
What’s at Risk? Penalties Plus…

Civil Monetary Penalties

Willful Neglect not 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
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
State Laws

Some States Have Less Stringent Law

• Alabama, New Mexico, and South Dakota have not enacted state breach notification laws.

Some States Have More Stringent Laws

• California requires breach notification within 5 business days.
Subpart D - Privacy

• HIPAA
  • 45 CFR 164 Subpart D – 164.501-164.532

• Topics
  • Uses and Disclosures
  • Patient Rights
  • Authorizations
  • Notice of Privacy Practices
  • Right to Request Information
  • Training

Items of Interest

• Policies, Procedures, Logs, Audit, Patient Forms, Internal Forms, Revision tracking
Subpart E - Breach

• HIPAA
  • 45 CFR 164 Subpart E – 164.402-164.414

• Topics
  • Notification to individuals
  • Notification to media
  • Notification to Secretary
  • Notification by a business associate
  • Law enforcement delay
  • Burden of proof

Items of Interest

• Policies, Procedures, Tracking/Revisions, Logs, Report, Training
Breach Notice

• **CEs must notify individuals of a breach without unreasonable delay (no case than 60 calendar days) from the discovery of the breach.**
  • Clock starts when the incident is first known; not when the investigation of the incident is complete.

• **Fewer than 500 individuals**
  • To individuals prior to 60 calendar days of discovery
  • To HHS prior to 60 days after the calendar year breach was discovered
  • To Covered Entity By Business associates prior to 60 calendar days of discovery

• **Greater than 500 individuals**
  • To individuals prior to 60 calendar days of discovery
  • To HHS immediately
  • To prominent medial outlet serving state or jurisdiction
  • To Covered Entity By Business associates prior to 60 calendar days of discovery
Subpart C - Security

- HIPAA
  - 45 CFR 164 Subpart C – 164.302-164.318
- Safeguards
  - Administrative Safeguards
  - Technical Safeguards
  - Physical Safeguards
  - Organizational Requirements
- Required/Addressable
Security – Key Items

Risk Analysis

- **Methodology** NIST, ISO, COBIT

Active Security Plan

CIA – Confidentiality, Integrity, Availability

Threat Groups

- Malicious Outsider
- Malicious Insider
- Human Error
- Environmental
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.
Risk Analysis

- Thorough and Accurate
- Follow Defendable Methodology
  - NIST recognized as “industry standard for good business practice with respect to securing EPHI” – OCR Guidance on Risk Analysis, July, 2010
- Update Regularly
- Must Contain Required Elements
  1. Scope – EPHI in all forms
  2. Data Collection – Where EPHI is stored
  3. Identify and Document Potential Threats and Vulnerabilities
  4. Assess Current Security Measures
  5. Determine Likelihood of Threat Occurrence
  6. Determine Potential Impact of Threat Occurrence
  7. Determine Level of Risk
  8. Finalize Documentation
  9. Periodic Review and Updates to the Risk Assessment
NIST Control Groups

- 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
Acute Care Audits

- Acute Care Meaningful Use Audits - CMS
  - 1 in 5 audited
  - Outsourced to Figliozzi & Co.
  - Desk audits to date

- Office of Inspector General – In-Depth Meaningful Use Audits

- Meaningful Use Stage 1 Security Requirement
  - Perform Risk Assessment

- Meaningful Use Stage 2 Security Requirement
  - Perform Risk Assessment
  - Address Encryption for EPHI Data at Rest
OCR HIPAA Audits

- Performed Test Audits in 2012
- Ramping Up for Audits in FY2015
- Currently Delayed – awaiting building of portal to accept information
- Not Outsourced
- Updating Audit Protocol
- Guidance
  - Use this time to get ducks in a row
Cloud

- Pros and Cons
- Private Cloud
- Public Cloud
- Business Associates
- Personal Cloud
Cyber Insurance

- Sample Application
Acute Care I.T. Priorities

- Meet Meaningful Use Requirements
- Implement System Upgrades
- Perform Risk Assessments each Reporting Period
- Meaningful Use Stage 2 Interoperability Requirement
  - Demonstrate exchange of structured care summaries of with other providers
- Meaningful Use Stage 3 Draft
Interoperability

- 10 Year Roadmap
- Privacy and Security in Fabric of Plan
- Acute/LTC
  - HIEs
  - Direct
  - C-CDA Consolidated-Clinical Document Architecture
  - Health Information Exchanges
Governance

• HIPAA Security Officer
• HIPAA Privacy Officer
• Executive Oversight
• Board Communication
Considerations

- Need to think beyond the EMR and mainstream billing systems:
  - Clinical photography - security of camera and stored images
  - Operational Registries, databases (even Excel spreadsheets)
  - Networked medical devices (e.g. smart pumps, etc.)
  - Laptops connected to diagnostic equipment

- Resident safety MUST be factored into your risk analysis and risk management process – always involve personnel from clinical, administrative and financial operations
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
HIPAA – Don’t Stop There

- Vendor/Business Associate Vetting
- Cyber Security Framework
Thank You!

Contact Information

John DiMaggio, Chief Executive Officer, Blue Orange Compliance
John.dimaggio@blueorangecompliance.com
614.270.9623

Cliff Mull, Partner, Benesch, Healthcare Practice Group
cmull@beneschlaw.com
216.363.4198