# Business Associates Are Under a Microscope –

# Are You Prepared?

Eric Fader and Susan Huntington

November 2, 2016

DAY PITNEY LLP

# Disclaimer

The information in this document is intended for educational purposes only and does not constitute legal advice.

Day Pitney is not recommending the adoption of any specific text for business associate agreements or other contracts.

DAY PITNEY LLP

# Day Pitney LLP

- In the rapidly evolving life sciences and healthcare industry, Day Pitney's interdisciplinary Healthcare and Life Sciences practice offers full, integrated services to address regulatory compliance, corporate and business, transactional, litigation, labor, employment and benefits, intellectual property, financial services, environmental, real estate, and tax needs. So whether you're in the business of biotechnology, nanotechnology, pharmaceuticals, medical devices, instrumentation and equipment, healthcare services, software, or support any of the foregoing, we can help every step of the way.

- Healthcare Law Blog site: http://healthcare.daypitney.com/

DAY PITNEY LLP

# Agenda

- Introduction – Focus on Business Associates
  - Enforcement actions
  - Inclusion in OCR Audits
  - Due Diligence by Covered Entities

- Business Associate Agreements
  - What can be negotiated
  - Added terms not required by HIPAA

- Cybersecurity Insurance
  - Who needs it?
  - What does it cover?

# Introduction: Why are we here?

- Volume and value of healthcare data
  - Use of data vendors, subcontractors
  - Data in medical devices

- Breaches involving BAs
  - Data from OCR shows increasing focus on BAs
    - "OCR wall of shame" – breaches involving PHI of 500 or more
  - Highly visible enforcement actions against Bas

- Covered entities are now performing due diligence

# HIPAA Background – How we got here

- HIPAA originally directed at covered entities
- BAs had only contractual liability to CEs under BAAs
- HITECH Act made BAs directly accountable to HHS
- Omnibus Rule (2013)
  - Confirmed direct OCR jurisdiction over BAs
  - Entity acting as BA is subject to regulation even without a BAA
  - Expanded definition of BA
  - Required amendments to BAAs by 9/14
  - Made CEs liable for civil money penalties for actions of agents (BAs)

# OCR's Increased Focus on Business Associates

- Phase 2 HIPAA Audit Program (began 4/16)
  - Includes both covered entities and business associates
  - Currently ongoing – desk audits with some on-site audits
- Cyber-Awareness Update, "Is Your Business Associate Prepared for a Security Incident?" (5/16)
- Guidance on cloud computing (10/16)

- Conclusion: Business associates are no longer below the radar! Must perform periodic risk assessments and train personnel, just as covered entities must.
  - Day Pitney's HIPAA Self-Assessment Tool is a user-friendly aid for both covered entities and business associates

# OCR Enforcement Actions

- Actions focused on covered entities involving BAAs
  - North Memorial Health Care (3/16, $1.55 million)
    - No BAA with major contractor
  - Oregon Health & Science University (7/16, $2.7 million)
    - Breach involved Google cloud-based document storage; no BAA
  - Raleigh Orthopaedic Clinic (4/16, $750,000)
    - Business partner received PHI without having BAA

- Actions focused on business associates
  - Care New England Health System (9/16, $400,000)
    - BAA had not been updated since 2005
  - Catholic Health Care Services of Archdiocese of Phila. (6/16, $650,000)
    - Theft of unencrypted IPhone; no mobile policy

# Expanded Definition of Business Associate

- "Conduit Exception" narrowed and clarified
  - Entity that maintains or transmits PHI for a CE is now a BA even if it doesn't access PHI. Applies to:
    - Cloud computing vendors
    - Conduits and switches that maintain PHI for any length of time
    - Server farms
    - Secure storage facilities (including physical warehouses)
- Subcontractors – "second tier" BA agreements
- "Workforce" exception

# Required Amendments to BAAs

- Subcontractors subject to same requirements
- Changes to breach notification requirements
- Limitations on remuneration for use of PHI
- Changes to individuals' access to PHI
- Other language changes – check with your legal counsel

# Negotiable Business Associate Agreement Provisions

- Indemnification
  - Only for any violation of BAA, or
  - More broadly, for data security-related incidents
- Limitation of liability
  - Carve-outs
- Cybersecurity insurance requirements
- Anything else that doesn't belong in a BAA

# Insurance Coverage

## Cyber Liability Coverage: Healthcare Sector

- According to a 2014 survey by Marsh Risk Management Research, the number of U.S.-based Marsh clients in the healthcare sector purchasing standalone cyber coverage increased from 45% in 2013 to 50% in 2014.
- The average cyber liability total limits purchased by companies in the same sector increased from $6.7 million in 2013 to $10.5 million in 2014.

SOURCE: MARSH MANAGEMENT RESEARCH, BENCHMARKING TRENDS: AS CYBER CONCERNS BROADEN, INSURANCE PURCHASES RISE (MARCH 2015)

# Insurance Coverage

| Coverage | Type of Losses |
|---|---|
| **First-party** | • Data loss<br>• Income loss<br>• Business interruptions costs<br>• System damage<br>• Costs to re-secure, recreate and/or restore data or systems<br>• Notification of affected parties, credit monitoring, call centers<br>• Cyber-extortion and cyber-terrorism |
| **Third-party** | • Claims for damages brought by customers, consumers or other businesses incurred as a result of breaches<br>• Defensive litigation services related to breaches (attorneys' fees and expert fees) |
| **Remediation** | • Public relations expenses<br>• Forensic services<br>• Regulatory official notification(s) |
| **Fines and penalties** | • Regulatory investigation expenses<br>• Civil judgments<br>• Fines and penalties |
| **Risk Management** | • Pre-breach/incident response planning services<br>• Mitigation of the risk of an information security incident |

# Stand-Alone Cyber Risk Insurance Coverage Considerations

- Application statements, reps and warranties*
- Notice timing
- Use of required public relations and/or notice provider
- Use of panel defense counsel

* *See Columbia Casualty v. Cottage Health System (2:15-cv-03432-DDP-AGR)*

DAY PITNEY LLP

# Thank You!

DAY PITNEY LLP

WOLF
& COMPANY, P.C.


# Business Associates are Under a Microscope – Are You Prepared?

Michael Kanarellis

November 2, 2016

# About Wolf & Company, P.C.

- Established in 1911
- Offers Audit, Tax, and Risk Management services
- Offices located in:
  - Boston, Massachusetts
  - Springfield, Massachusetts
  - Albany, New York
  - Livingston, New Jersey
- Over 200 professionals

*As a leading regional firm founded in 1911, we provide our clients with specialized industry expertise and responsive service.*

# IT Assurance Services

- HIPAA and Regulatory Audits
- NIST/ISO/PCI/COBIT Reviews
- Information Privacy Review
- Application Security Review
- Vulnerability Assessments
- Social Engineering Assessment
- Risk Assessments
- Business Continuity Planning (BCP)
- Incident Response Planning (IRP)
- Penetration Testing
- Internal IT Audit Support (SOX 404)
- SSAE16 & SOC 2 Assurance

# Objectives

- Understand the current regulatory environment
- Become aware of which **regulatory** audits you may be subject to
- Understand which **industry** audits you may be subject to

# Current Regulatory Environment

- Increase in reported healthcare data breaches
- Higher fines from the OCR
- Greater regulatory oversight on Vendor Due Diligence
  - Hospitals are ramping up their Vendor Management Programs
- Breaches are more likely to occur with **business associates** (BAs)
  - HIPAA Final Omnibus Rule addresses BAs
- Prevalence of healthcare organizations outsourcing business functions to hosted and cloud BAs
- **Greater need for 3rd party assurance reports**

# Healthcare Business Associate Audit Areas

- HIPAA Security Analysis and Risk Assessment
- Service Organization Controls Audit: SOC 2 Audit
- Payment Card Industry Data Security Standard: PCI DSS
- Health Information Trust Alliance Audit: HITRUST
- Penetration Testing

# HIPAA Security Analysis

- The Security Rule: 45 CFR Part 160 and Subparts A and C of Part 164
- Regulatory mandate for BAs that house or transmit ePHI
- Needs to be risk based
- First define operating controls around Administrative, Technical and Physical Safeguards of ePHI
  - NIST Special Publication 800-66
- Once controls are defined and control gaps are identified create Risk Assessment
  - NIST Special Publication 800-30

# Service Organization Control Report (SOC)

- SOC 1 Report
  - Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting (SSAE No. 16)
- SOC 2 Report
  - Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, and/or Privacy

# Trust Services Principles

- **Security** – System is protected against unauthorized access (both physical and logical)
- **Availability** – System is available for operation and use as committed or agreed
- **Processing Integrity** – System process is complete, accurate, timely, and authorized
- **Confidentiality** – Information designed as confidential is protected as committed or agreed
- **Privacy** - Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the entity's privacy notice, and with criteria set forth in GAPP

# Security Principle

- Security Policies
- Incident Response Plan
- Change Control
- Risk Assessment on threats to security
- Logical Access
- Physical Access
- VPN, Firewall, Network Services, IDS/IPS
- Anti-Virus
- Encryption
- Vulnerability Management and Assessments
- Log Monitoring
- Review of Environmental, Regulatory, and Technological Changes

# Availability Principle

- Availability Policies
- Change Control
- Risk Assessment on threats to availability (internal or external physical environment)
- Environmental Controls
- Backup and Recovery
- Disaster Recovery Plan
- Incident Response Plan
- Network Performance and System Process Monitoring

# Type 1 vs. Type 2

- **Type 1**
  - Report on management's description of a service organization's system and the suitability of the design of controls
  - **As of a specified date**

- **Type 2**
  - Report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls
  - **Throughout the specified period**

# Elements of a SOC 2 Report

- **Section 1: Service Auditor**
  - Independent Service Auditor's Report (Opinion Letter)
- **Section 2: Service Organization**
  - Service Organization's Assertion
- **Section 3: Service Organization**
  - Description of a Service Organization's System
  - Control Objectives and Control Activities (SOC 1) / Trust Services Principles and Criteria and Controls (SOC 2)
  - Complementary User Entity Controls
- **Section 4: Service Auditor (Type 2 Only)**
  - Independent Service Auditor's Description of Tests of Controls and Results
- **Section 5: Service Organization**
  - Additional information provided by the service organization

# PCI DSS Audit

- PCI DSS is a standard for credit card data security, established in 2004 by the major payment card brands – Visa, MasterCard, American Express, Discover and JCB. First major revision in 2006
- Contains series of more than 280 security controls designed to protect credit card data
- PCI DSS is broken down into 12 major requirements
- Overall goal of an assessment is to reduce Credit Card Environment (CDE) scope on the network!

# PCI DSS Audit (cont.)

✓ **Build and Maintain a Secure Network**

1) Install and Maintain a firewall configuration to protect cardholder data
2) Do not use vendor-supplied defaults for system passwords and other security parameters

✓ **Protect Cardholder Data**

3) Protect stored cardholder data
4) Encrypt transmission of cardholder data across open, public networks

# PCI DSS Audit (cont.)

✓ **Maintain a Vulnerability Management Program**

5) Protect all systems against malware and regularly update anti-virus software and programs

6) Develop and maintain secure systems and applications

✓ **Implement Strong Access Control Measures**

7) Restrict access to cardholder data by business need to know

8) Identify and authenticate access to system components

9) Restrict physical access to cardholder data

# PCI DSS Audit (cont.)

✓ **Regularly Monitor and Test Networks**

10) Track and monitor all access to network resources and cardholder data

11) Regularly test security systems and processes

✓ **Maintain an Information Security Policy**

12) Maintain a policy that addresses information security for all personnel

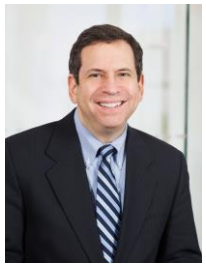
# HITRUST Validated Audit

- What is HITRUST CSF
  - Certifiable framework for the healthcare industry
  - Based on ISO 27001
  - Integrates HIPAA, HITECH, NIST 800-53, ISO 27001, PCI DSS, FTC, COBIT and State Laws
  - Tailorable based on the organization
- Assessment methods
  - Self Assessment
  - Validated Assessment
  - SOC 2 Plus HITRUST
  - SOC 2 Plus HITRUST Plus HITRUST Certification

# Penetration Testing

- External Penetration Testing
- Internal Penetration Testing
- Wireless Penetration Testing
- Application Penetration Testing

# Thank You & Questions!



**Eric Fader**
Counsel
Day Pitney LLP
EFader@daypitney.com

**Susan Huntington**
Counsel
Day Pitney LLP
SHuntington@daypitney.com

**Michael E. Kanarellis**
IT Assurance Senior Manager
617-428-5408
mkanarellis@wolfandco.com