EFFECTIVE STRATEGIES FOR MANAGING BUSINESS ASSOCIATE RELATIONSHIPS

June 2016

FOLEY & LARDNER LLP

MOSS-ADAMS LLP
Certified Public Accountants | Business Consultants

The material appearing in this presentation is for informational purposes only and should not be construed as advice of any kind, including, without limitation, legal, accounting, or investment advice. This information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although this information may have been prepared by professionals, it should not be used as a substitute for professional services. If legal, accounting, investment, or other professional advice is required, the services of a professional should be sought.

Speaker Introductions

Shirley Komoto
Director, Moss Adams LLP
Shirley.Komoto@mossadams.com

Leeann Habte
Senior Counsel, Foley & Lardner LLP
Lhabte@Foley.com

FOLEY
FOLEY & LARDNER LLP

MOSS-ADAMS LLP 3

Agenda

- Recent Changes and Focus on Business Associates
- Phase 2 Audit Protocol Focus on Business Associates
- Decision Framework for Identifying Business Associates
- Business Associate Relationships
- OCR Emphasis on Business Associate Relationships
- Auditing and Monitoring Business Associates
- Case Examples
- Last Thoughts
- Question and Answer Session

FOLEY
FOLEY & LARDNER LLP

MOSS-ADAMS LLP 4

Recent Changes and Focus on Business Associates

- The Office for Civil Rights (OCR) has launched Phase 2 of its audit program targeting common areas of noncompliance, including **HIPAA* Business Associate relationships.**
- The OCR revised audit protocols, updated to incorporate changes made under the HIPAA Omnibus Final Rule, were released http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html for Phase 2.
- Major compliance issues are likely to result in expanded investigations and could result in settlements or monetary penalties.

***HIPAA = Health Insurance Portability and Accountability Act of 1996**

FOLEY
FOLEY & LARDNER LLP

MOSS-ADAMS LLP 5

Phase 2 Audit Protocol Focus on Business Associates

Questions the OCR will ask:

- Does the Covered Entity have contracts with Business Associates?
- Do the Business Associate Agreements (BAAs) contain all the required elements?
- **How does Management identify and engage Business Associates**?
- Do the BAAs involve onward transfer of PHI to subcontractors?
- Has the Covered Entity become aware of a pattern or practice of the Business Associate that constitutes a material breach or violation of the Business Associate's obligation?

FOLEY
FOLEY & LARDNER LLP

MOSS-ADAMS LLP 6

Decision Framework for Identifying Business Associates

Is a Business Associate Agreement required?

- Step 1: Does the arrangement involve PHI?
- Step 2: Are the functions or services defined as Business Associate functions/services?
- Step 3: Are the function or services provided for or on behalf of the Covered Entity?

Business Associate Decision Framework: Step 1

Does the arrangement **involve PHI**?

> *PHI is individually identifiable health information maintained in any form (including demographic information) which relates to an individual's past, present, or future physical or mental health or condition; the provision of health care to the individual; or payment for the provision of health care to the individual.*

Does the contractor **create, receive, maintain, transmit, or access** PHI?

Exception: Is the use or disclosure **incidental**?

Business Associate Decision Framework: Step 2

Are the functions or services defined as **Business Associate functions/services**, such as the following?

- Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, financial services.
- Claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, certain patient safety, billing, benefit management, practice management, repricing services, or other activities regulated by HIPAA.
- Data transmission services that require access on a routine basis to PHI.
- Personal health records.

Exceptions:

- Is the disclosure to a health care provider for treatment?
- Is the disclosure (if by a health plan) to the health plan sponsor?
- Is the disclosure to a government agency for eligibility determinations or enrollment in a government health plan?

Business Associate Decision Framework: Step 3

Are the services being performed **for or on behalf of the** Covered Entity?

Exceptions:

- Is the function or service being performed in the capacity of a Workforce member?
- Is the function or service being performed by a member of an Organized Health Care Arrangement in which the Covered Entity participates?
- Is the service performed for or on behalf of patients?

Business Associate Relationships

BAAs are not necessary with:

- Entities that do not access, create, receive, maintain, or transmit PHI
- Conduits for PHI (ISPs)
- Entities who receive only encrypted PHI
- Health Care Providers who receive PHI to treat patients
- Members of the Covered Entity's Workforce
- Members of an Organized Health Care Arrangement
- Entities who provide services on behalf of the patient

OCR Emphasis on Business Associate Relationships

Two of the four most recent civil monetary penalties involved failure to implement BAAs.

Implementing BAAs after the contract begins and PHI is disclosed is risky:

- North Memorial Medical Center was fined $1.55 Million on March 16, 2016, and entered into a Resolution Agreement.
- North Memorial entered into a BAA six months after it began providing PHI to Accretive Health, an entity that provided billing services.
- There was a breach of PHI during that six-month period, when no BAA was in place.
- The result was a Civil Monetary Penalty and Corrective Action Plan.

OCR Emphasis on Business Associate Relationships (cont.)

Corrective Action Plan Requirements:

- Responsibility for BAAs
- Identification of Business Associates
- Executing Agreements
- Documentation
- Minimum Necessary

FOLEY
FOLEY & LARDNER LLP

Auditing and Monitoring Business Associates

	Issues	Controls
Oversight	• Leadership did not understand or buy in to the Business Associate process, too much work, insufficient staff	• Designate a knowledgeable leader • Require check off before disclosing PHI to any third party • Implement policies and procedures • Ensure sufficient resources
Awareness	• Management did not actively support • Purchasers and approvers did not understand requirements and risks • Staff did not know when a BAA was required	• Communicate policies and procedures • Educate personnel authorized to issue POs or sign contracts regarding identifying BAs and associated risks and controls • Integrate requirements and audit rights into BAAs • Educate vendors/contractors and subcontractors

FOLEY
FOLEY & LARDNER LLP

Auditing and Monitoring Business Associates (cont.)

	Issues	Controls
Inventory	• No central inventory of vendors, contractors and other third parties • Lack of support to identify and centralize	• Require a central inventory • Confirm PO-vendors, affiliates, others are included • Implement a process to ensure completeness and accuracy
Risk Analysis	• Insufficient information about third parties' access and use of PHI • Threats and vulnerabilities of the data exist, not well understood • Third-party safeguards are unknown	• Conduct periodic assessment of threats and vulnerabilities of PHI • Document the thought process and results • Review and adjust existing safeguards and controls to address risks • Implement a review process by leadership to confirm both risks and controls

Auditing and Monitoring Business Associates (cont.)

	Issues	Controls
Mitigation	• Identified gaps were not addressed with action • PHI may have been released without timely BAA	• Ensure leadership oversight and monitoring • Task specific individuals for mitigating actions • Ensure completeness and accuracy • Document specific actions for risk areas • Business Associate audit work plan • Approval and BAA **BEFORE DISCLOSURE** of PHI or ePHI • Third-party due diligence processes • Training • Monitoring mitigation • Report to leadership and governing body

Auditing and Monitoring Business Associates (cont.)

	Issues	Controls
Audit	• Inventory incomplete • Risk analysis inaccurate • Policies and controls not communicated or implemented • Control performers not sufficiently trained • No assurance for leadership that BAAs are properly managed and controlled	• Assess process to inventory third-parties • Review processes around disclosures to external parties and related BAAs • Confirm document retention is consistent with requirements • Verify management's auditing and monitoring over BA and related subcontractor compliance • Verify the process for terminating third-parties

Case No. 1: Data Transfer/Destruction

Situation:

A provider group practice that operates clinics and a surgery center released x-ray files and related PHI of 17,300 patients to an entity to transfer the images to electronic media for the group practice, in exchange for harvesting the silver from the x-ray films.

Questions:

- Is a BAA required?
- What internal controls would you expect to see to identify this type of vendor? What if the agreement was made via a purchase order as opposed to a contract? What if it was an oral agreement?
- Is transfer of PHI prior to implementation of a BAA reportable to OCR as a breach?

Case No. 2: Filming/Public Relations

Situation:

A health care provider uses the services of a contract film crew to produce training videos or public relations materials for the provider. Filming is done within the health care provider's facility and patients may be interviewed or PHI peripherally captured during filming.

Questions:

- Is a BAA required?
- Can the crew enter a treatment room?
- Is patient authorization required from patients whose PHI is included, even if a BAA is in place?
- What additional controls might be necessary to ensure only permissible PHI is disclosed in materials?
- What other concerns would you have?

Case No. 3: Research

Situation:

A not-for-profit biomedical research institute is a wholly owned subsidiary of a large health system with 21 hospitals and over 450 patient facilities and physician practices. The Institute conducts research on behalf of the health system. A laptop was stolen from an employee's car, containing ePHI from 13,000 patients and research participants including dates of birth, addresses, social security numbers, diagnoses, lab results, medical, etc.

Questions:

- Is a BAA required?
- Is the research institute a Covered Entity? Is it a separate Covered Entity from the health system?
- What are the issues that you see with the relationship between the parties?
- What controls are appropriate for these circumstances?

Case No. 4: Mhealth Applications

Situation:

A mhealth (mobile health) application for individuals with a chronic disease is provided to patients of a health care provider via prescription. The practice does not pay for the application, but physicians have access to information generated by the application and logged by patients via a web portal. Physicians can update instructions for patients for providing services.

Questions:

- Is a BAA required, or is this a disclosure for treatment?
- What internal controls should be in place to identify and evaluate this type of arrangement?
- What if the mobile device manufacturer is also a Covered Entity health care provider?
- What are the factors to consider?

Case No. 5: HIE Vendors/HISPs

Situation:

A provider enters into an agreement with a health information services provider (HISP). The HISP vendor does not maintain ePHI. ePHI is encrypted during transmission.

Questions:

- Is a BAA required?
- Does vendor have routine access, or is it a conduit?
- What internal controls are needed to identify and evaluate such arrangements?
- What are the factors to consider?

***HIE = Health Information Exchange**

Case No. 6: Wellness Application

Situation:

As part of its wellness program, a Covered Entity employer offers reduced premiums to employees who meet certain health and fitness goals. The employer provides free subscription to online fitness application to employees. Health scores are transmitted to employer and group health plan.

Questions:

- Is a BAA required?
- What controls should be in place to identify and evaluate such vendors?
- What are the factors to consider?

Case No. 7: Case Management/Care Coordination

Situation:

Health plan hires a case management service to identify diabetic and pre-diabetic patients at high risk of non-compliance and recommend optimal interventions to those patients.

Questions:

- Is a BAA required?
- Is it health care operations or treatment?
- What internal controls are necessary to identify and evaluate such arrangements?
- What are the factors to consider?

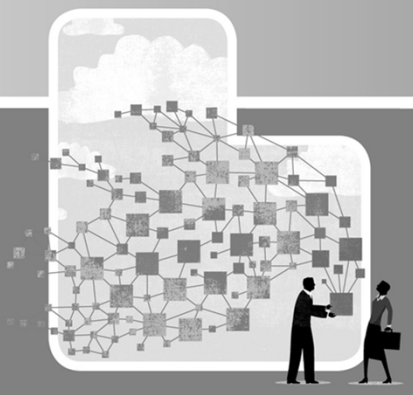
Last Thoughts

- What other arrangements may vary with respect to whether a BAA is required?
  - Website developer
  - Medical Director for a hospital
- What is an acceptable level of diligence over your Business Associates and their subcontractors?
- What are the risks/considerations regarding offshore contracting, data hosting in the cloud?
- What are the liability considerations in a Business Associate arrangement?

FOLEY
FOLEY & LARDNER LLP

MOSS-ADAMS LLP 25

Question and Answer Session



FOLEY
FOLEY & LARDNER LLP

MOSS-ADAMS LLP
Certified Public Accountants | Business Consultants