Responsibilities and Rights of Subcontractors in the Compliance Chain

The 23rd National HIPAA Summit
The Leading Forum on Healthcare EDI, Privacy, Confidentiality, Data Security and HIPAA Compliance

Phyllis A. Patrick, MBA, FACHE, CHC, CISM

The 23nd National HIPAA Summit

March 17, 2015

Topics

- Roles and Responsibilities of Subcontractors in the Compliance Chain
- Review of HIPAA Omnibus (Final) Rule Requirements for Subcontractors
- Scenarios: The Complexity of Relationships
- Subcontractor Due Diligence Checklist

Roles and Responsibilities of Subcontractors in the Compliance Chain

General Provisions: Definitions - Subcontractor - § 160.103

- Definition of "business associate" modified to provide that subcontractors of a covered entity, i.e., those persons that perform functions for or provide services to a business associate other than in the capacity as a member of the business associate's workforce, are also business associates to the extent that they require access to protected health information.
- "Subcontractor" defined as a person who acts on behalf of a business associate, other than in the capacity of a member of the workforce of such business associate.
- The definition applies to an agent or other person who acts on behalf of the business associate, even if the business associate has failed to enter into a business associate contract with the person.

HHS – Omnibus Rule

"[W]e believe that making subcontractors directly liable for violations of the applicable provisions of the HIPAA Rules will help to alleviate concern on the part of covered entities that protected health information is not adequately protected when provided to subcontractors."

"Everybody is a Contractor"

- *Modern Healthcare's Annual Outsourcing Surveys* indicate increasing use of contractors to perform a diversity of functions.
- More companies have increased their participation in health care, seen as a "new and lucrative market."
  - ✓ Revenue Cycle Management
  - ✓ Information Technology Services
  - ✓ Support Services (Dietary, Engineering)
  - ✓ Therapy Services
  - ✓ Medical Equipment
  - ✓ Professional Services (Anesthesiology, Emergency Department, Radiology, Laboratory)
  - ✓ Others

Top 100 Contractors Report – U.S. GSA

Top Contractors FY2013 by Dollars Spent

1 Lockheed Martin Corporation
2 The Boeing Company
3 Raytheon Company
4 Dynamics Corporation
5 Northrop Grumman Corporation
6 SAIC Inc.
7 Huntington Ingalls Industries
8 L-3 Communications Holdings Inc.
9 United Technologies Corporation
10 BAE Systems PLC
11 McKesson Corporation
12 Bechtel Group Inc.
13 Veritas Capital Fund
14 Humana Inc.
15 Computer Sciences Corporation

http://en.wikipedia.org/wiki/Top_100_Contractors_of_the_U.S._federal_government

In Fiscal Year 2011, the top five departments by dollars obligated were the Department of Defense ($373.6 billion), Department of Energy ($25.1 billion), Health and Human Services ($19.3 billion), Department of Veteran Affairs ($17.4 billion), and NASA ($15.4 billion).

Examples of Subcontractor Functions

- Staffing Companies
- Shredding/Disposal Companies
- Companies/Individuals who create de-identified data
- IT Companies (e.g., electronic medical records, specialty systems, infrastructure development, network management, software and data base development and management, project management, security functions, outsourcing)

Entities that Use Subcontractors

- Hospitals and Health Systems
- Physician Groups
- Information Technology Vendors
- Health Insurance Companies
- Health Information Exchanges
- Pharmaceutical Companies
- Device Companies

HIPAA Requirements for Subcontractors

Responsibilities of Subcontractors

- Security Rule
- Privacy Rule (some sections)
- Breach Notification Rule
- Enforcement Rule

The Security Rule and the Privacy Rule require covered entities, business associates and subcontractors to implement policies, ensure accountability fir compliance, limit access to PHI, conduct workforce training and safeguard PHI.

Security Rule Standards: Administrative Safeguards

SECURITY MANAGEMENT PROCESS	164.308(a)(1)(i)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
ASSIGNED SECURITY RESPONSIBILITY	164.308(a)(2)	(R)
WORKFORCE SECURITY	164.308(a)(3)(i)	Authorization and/or Supervision (A) Workforce Clearance Procedure (A) Termination Procedures (A)
INFORMATION ACCESS MANAGEMENT	164.308(a)(4)(i)	Isolating Health Care Clearing House Functions (R) Access Authorization (A) Access Establishment and Modification (A)

Security Rule Standards: Administrative Safeguards (Cont'd)

SECURITY AWARENESS AND TRAINING	164.308(a)(5)(i)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
SECURITY INCIDENT PROCEDURES	164.308(a)(6)(i)	Response and Reporting (R)
CONTINGENCY PLAN	164.308(a)(7)(i)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedures (A) Applications and Data Criticality Analysis (A)
EVALUATION	164.308(a)(8)	(R)
BUSINESS ASSOCIATE AGREEMENTS/ CONTRACTS AND OTHER ARRANGEMENTS	164.308(a)(8)(b)(1)	(R)

Security Rule Standards: Physical Safeguards

FACILITY ACCESS CONTROLS	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
WORKSTATION USE	164.310(b)	(R)
WORKSTATION SECURITY	164.308(c)	(R)
DEVICE AND MEDIA CONTROLS	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)

Security Rule Standards: Technical Safeguards

ACCESS CONTROLS	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic logoff (A) Encryption and Decryption (A)
AUDIT CONTROLS	164.308(b)	Integrity (A) Mechanism to Authenticate Electronic Protected Health Information (A) Transmission Security (A) Integrity Controls (A) Encryption (A)

Privacy Rule Standards: BAs and Subcontractors

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION	164.502(a)(3) 164.502(a)(4) 164.502(a)(5)	Permitted uses and disclosures, required uses and disclosures, prohibited uses and disclosures by business associates. Sale of protected information.
DEFINITIONS (BUSINESS ASSOCIATE)	164.103(1) – (4)	Definition of Business Associate.
NOTIFICATION BY A BUSINESS ASSOCIATE	164.410	Breaches treated as discovered, timeliness of notification, and content of notification.
LAW ENFORCEMENT DELAY	164.412	Applies to covered entities and business associates.

Privacy Rule Standards: BAs and Subcontractors (Cont'd)

MINIMUM NECESSARY	164.502(b)	Business associate must make reasonable efforts to limit PHI to minimum necessary to accomplish the intended purpose of the use, disclosure or request.
USES AND DISCLOSURES OF DE-IDENTIFIED DATA	164.502(d)(1) and 164.502(d)(2)	Uses and disclosures to create and use de-identified information
DISCLOSURES TO BUSINESS ASSOCIATES	164.502(e)(1) and 164.504(e)(1)(i)	Covered entity may disclose and may allow BA to create, receive, maintain, or transmit PHI on its behalf. BA may disclose PHI to a subcontractor and may allow subcontractor to create, receive, maintain, or transmit PHI on its behalf, if BA receives satisfactory assurances that subcontractor will appropriately safeguard the information.

Privacy Rule Standards: BAs and Subcontractors (Cont'd)

BUSINESS ASSOCIATE CONTRACTS	164.504(e)(2)	Contract required. Must establish permitted uses and disclosures of PHI by BA. Requirements of subcontractors delineated. BA must make information available for accounting of disclosures. BA MUST return or destroy all PHI at termination of contract. BA must have BAAs with subcontractors and all provisions apply equally to subcontractors.
WORKFORCE TRAINING AND MANAGEMENT	160.103 and 164.530(b)	Requirements for training workforce members of BAs and subcontractors.
SANCTIONS	164.530 (e)	Sanctions policy for workforce members required.

Scenarios

Scenario 1: Behavioral Health Network

- 58 providers (large and small) formed a community association/network with the goal to improve behavioral health and community services for residents of a major metropolitan county.
- A major pharmaceutical company is providing electronic medical record services, data base development and infrastructure services through contractual relationships with several software and data base development vendors. Other companies assisting in the project (marketing development, community outreach, and other services) are subs to some of the IT vendors.
- Approximately 75 – 80 different companies involved.

Scenario 1: Questions

- Must HIPAA Regulations be met? If yes, by which entities?
- Which entity is in charge of the project?
- Who is responsible for contract and BAA development, maintenance, and monitoring for each entity and for the project as a whole?
- In the event of a breach by a subcontractor, who is responsible for investigating, reporting, mitigating, etc?

Scenario 2: EMR Vendor and Staffing Company

- A national, successful EMR vendor, with many hospital and physician group clients, hires consultants from a staffing company to assist in EMR development, implementation and project management. Consultants are hired based on past accomplishments and experience with the EMR software and implementations.
- Consultants perform their work at the client site and are required to provide their own computers. Consultants are generally on the job for at least two years.
- The staffing company has seen its share of heath care providers increase in past five years and plans to expand further into this market.

Scenario 2: Questions

- Since the EMR Vendor is a business associate to its clients, what are its obligations to assure that the staffing company, a subcontractor, fulfills its HIPAA obligations?
- Should the consultants be trained in policies and procedures of the business associate, the covered entity or both?
- If a consultant becomes aware of a possible data breach, what are the individual's obligations for reporting to management and to the business associate?
- Rather than making consultants responsible for their own equipment, should the BA provide and manage all equipment used on site? Pros and cons?

Relationship Management

Position and Rights of Subcontractors

- Contracts and Business Associate Agreements are limited.
- Should subcontractors add language in their BAAs with business associates to detail the responsibilities and obligations of the BAA and the covered entity?
- What about costs associated with breach mitigation – should this be spelled out in agreements?
- If a covered entity imposes additional burdens on a BA (short notification requirements, specific encryption requirements, audits, etc.) how does the BA respond to this and how does this affect the subcontractor?

Subcontractor Due Diligence Checklist

- Review and understand your obligations as a subcontractor.
- When entering into an agreement with a business associate to provide services on behalf of a covered entity, be clear as to the roles and responsibilities of each subcontractor involved in the engagement.
- Review contracts and BAAs with legal counsel.
- Develop model BAA to assure that subcontractor rights are addressed and included in agreements.

Subcontractor Due Diligence Checklist (Cont'd)

- Develop and implement policies and procedures for HIPAA requirements (Security, Privacy, Breach Notification Rules). If specific standards of a Rule do not apply directly, document the reason.
- Request and review policies and procedures of Business Associate(s). Request clarification if required. Be clear as to expectations and responsibilities of all parties!
- Communicate with BA and review obligations and expectations and responsibilities of each party.
- Review and sign new BAAs as required.

Subcontractor Due Diligence Checklist (Cont'd)

- Conduct risk analysis and develop risk mitigation plans, as required by HIPAA Security Rule. Update as appropriate.
- Develop and provide/update HIPAA training programs for all subcontractors. Document training for each subcontractor/consultant. Make sure training is relevant!
- Request and have all consultants participate in BA training programs and CE training programs, including participating while on site.
- Periodically review organizational strategy and HIPAA Compliance Program.

PHYLLIS PATRICK + Associates

Security | Privacy | Culture

phyllis@phyllispatrick.com
914-417-8592
www.phyllispatrick.com