HIPAA Compliance and Non-Business Associate Vendors: Strategies and Best Practices

July 14, 2015

William J. Roberts, Esq.

Forward Thinking Healthcare Solutions

It's What We Do

SHIPMAN & GOODWIN® LLP
COUNSELORS AT LAW

HEALTHCARE LAW

@SGHealthLaw

Key Issues

- Which vendors are HIPAA business associates?
- Should you be concerned about those vendors that are not business associates?
- How should your organization manage the risks posed by non-business associate vendors?

About HIPAA

- HIPAA is a federal law that governs the use, disclosure and safeguarding of individually identifiable health information.
- One of many state and federal laws that govern information held by health care providers and health plans. Others include:
  - Substance abuse confidentiality regulations; and
  - State personal information laws.

When Does HIPAA Apply?

- HIPAA applies to most health care providers and health plans ("covered entities") and certain third parties who use PHI to provide services for or on behalf of the covered entity ("business associates").
  - Business associates often include attorneys, consultants, IT firms, shredding companies and other vendors.
- Exceptions may include:
  - health care services provided by schools or colleges/universities; or
  - certain health care providers that are cash-only.

Identifying Business Associates

- Any individual or organization that either:
  - Creates, receives, maintains, or transmits PHI on behalf of a covered entity for a function or activity regulated under HIPAA, such as claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, or repricing; or
  - Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity, if the service involves the disclosure of PHI.
- Those who store or otherwise maintain PHI.
- Certain data transmission services.
- Certain personal health record vendors.
- Subcontractors.

Identifying Business Associates

- Who is not a business associate?
  - Workforce members.
  - Parties receiving PHI through litigation proceedings.
  - Recipients of PHI disclosed when required or permitted by law, such as disclosures to law enforcement or state agencies.
  - Typically, cleaning/food services.
- Managing Business Associates
  - Keep a file of all business associate agreements – make sure they are executed and kept current.
  - Periodically review vendors to see if any business associate agreements are missing.

Data Transmission Services

- Data Transmission Services
  - Business associates include health information organizations and e-prescribing gateways.
  - To qualify as a business associate, the data transmission service must have "routine" access to the PHI it is transmitting.
  - The "conduit exception" – if an entity is simply acting as a pass-through with no routine access, not a business associate.
    - Examples include telephone company, UPS and courier services.

Personal Health Record Vendors

- Personal Health Record vendors may be a business associate.
  - Not all vendors of personal health records will be your business associate.
  - Fact-specific determination.
  - Key: If you are hiring a vendor to provide a personal health record service for your patients, the vendor is likely a business associate.

Entities that "Maintain" PHI

- The definition of business associate includes entities which "maintain" PHI on behalf of a covered entity, even if the entity does not access or view the PHI.
  - Includes paper record and cloud storage firms.
  - Whether the vendor accesses your PHI is irrelevant.
- Entities that "temporarily" maintain or store PHI.
  - If the conduit exception applies, no business associate relationship (i.e. UPS or an internet service provider temporarily storing PHI while transmitting it, while not routinely accessing it).
  - Otherwise, temporary storage would create a business associate relationship (e.g. a shredding company which temporarily maintains PHI prior to shredding it).

Subcontractors

- The definition of "business associate" includes subcontractors that create, receive, maintain, or transmit PHI on behalf of a business associate.
  - Excludes workforce members.
  - Examples:
    - Hospital engages a consulting firm to advise the hospital on quality and patient safety issues, and provides PHI to the consulting firm as part of the engagement.
    - Consulting firm in turn provides the PHI to a third party copy center, off-site shredding firm and cloud storage email platform.
- HIPAA applies to all downstream subcontractors in the same manner as it applies to the business associates that directly contract with covered entities.

What About Everyone Else?

- A vendor is a business associate if it falls under one of the following categories:
  - Creates, receives, maintains, or transmits PHI on behalf of a covered entity for a function or activity regulated under HIPAA.
  - Stores or otherwise maintains PHI.
  - Provides certain data transmission services.
  - Certain personal health record vendors.
  - Subcontractors.
- Not all vendors will be business associates – how should you handle these vendors?

Polling Question #1

Non-Business Associate Vendors

- Generally, a vendor is not a business associate if it does not receive, use, disclose or maintain PHI.
- Examples:
  - IT vendor will have access to hospital information systems to install, update or maintain malware protection.
  - Cleaning service with access to staff offices, medical record rooms or other areas in which PHI may exist.
  - A software company which licenses a locally hosted program which utilizes or processes PHI.
  - A consultant who is granted limited access to quality, compliance or other internal reports which include only aggregate information.

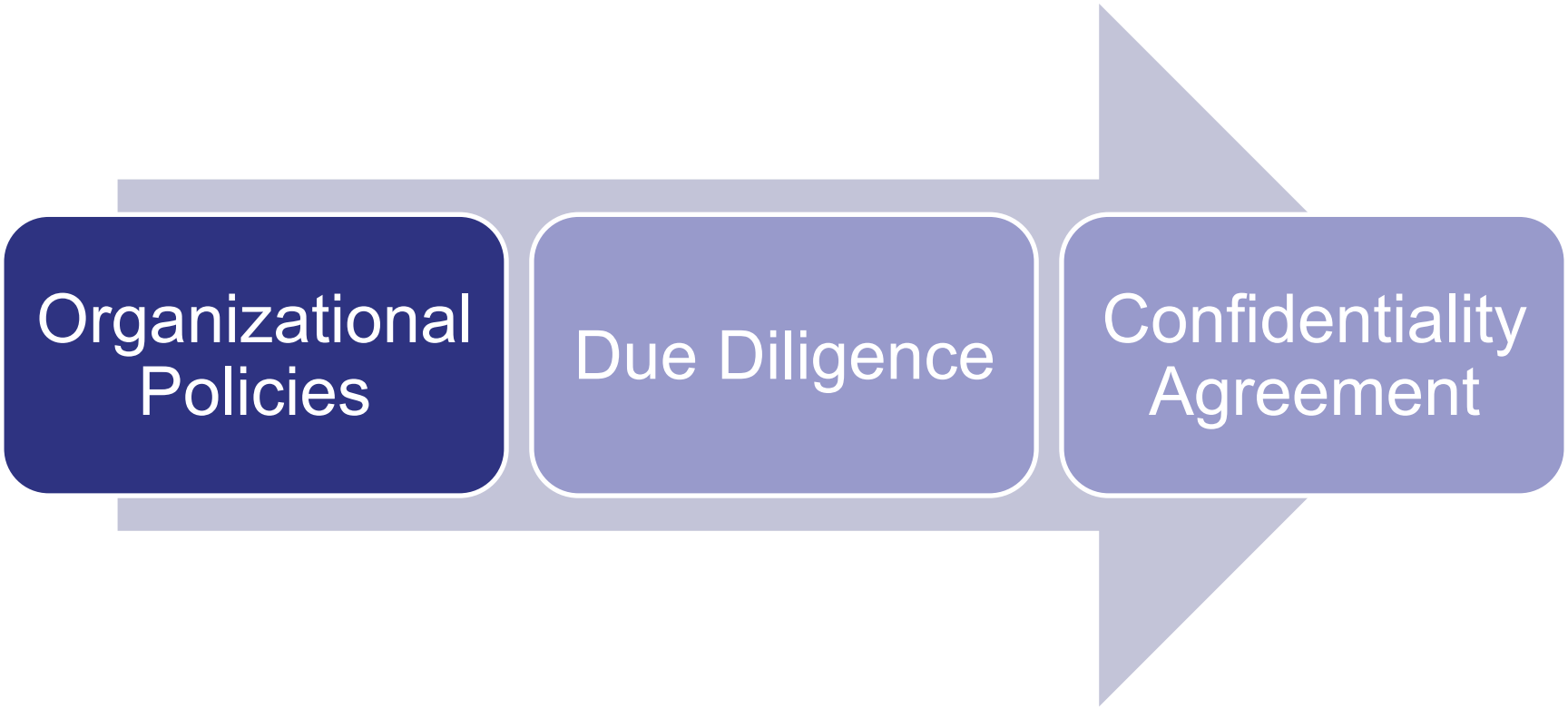
Non-Business Associate Vendors

- Despite not being subject to HIPAA, your organization's relationship with a non-business associate vendor may entail significant risk for your organization. Consider:
  - Data Access: What type of data will the vendor have access to? Even if not PHI subject to HIPAA, confidentiality concerns may nevertheless exist under state law or concerns with proprietary information.
  - Access to Premises: Will the vendor have access to your premises or information systems? If so, would that access enable the vendor to access PHI?
  - Incidental Use or Disclosure: Will the vendor have incidental use or disclosure of PHI?
- Key Point: ***Don't ignore a vendor simply because it's not a business associate!***

Example of Non-BA Incident

- Community health center engages a local IT security firm to install patches. Parties agree that vendor is not a business associate. While in the center's information system, a newly hired vendor employee stumbles upon locally maintained patient and employee records. Bored, he starts reviewing the records and finds a former classmate of his. He copies the records to a USB drive and emails the records to the former classmate. Several weeks later, the former classmate contacts the state AG and says "look what the health center gave [the employee] access to."
- Vendor employee failed to appreciate the seriousness of the access (no privacy training provided), was under no obligation to report the access to employer, and Vendor had no obligation to notify, indemnify, reimburse or cooperate with the center.
- Resulted in HIPAA and state law violations and an extensive corrective action plan.

3 Part Strategy for Non-Business Associates



Organizational Policies

- Don't limit your privacy and security policies to only HIPAA compliance – while important, HIPAA is not the only privacy and security concern a covered entity or business associate should have.
  - Proprietary information and trade secrets.
  - State privacy laws.
- Ensure that policies apply to all vendors, and not merely those subject to HIPAA.
- Revisit policies regarding access to premises and information systems.
- Determine when your organization requires a non-business associate to enter into a confidentiality agreement.

Polling Question #2

Due Diligence

- Consider implementing a vendor screening tool as part of your contracting process.
  - Obtain privacy and security information and assurances from a potential vendor prior to entering into negotiations.
  - Receive comfort that a vendor who will have access to your premises or information systems is cognizant of privacy concerns, takes privacy seriously and has a privacy and security plan in place.
  - Use vendor screening tool as a way to periodically monitor vendor and remind vendor of privacy and security expectations (i.e. annual or bi-annual re-certification).
  - Make privacy and security a factor when choosing vendors.

Confidentiality Agreements

- In many instances, a covered entity or business associate may desire to require the vendor to agree to a confidentiality agreement or contract clause.
- The extent and scope of such requirements should be based upon the risk to the organization.
- Key Terms:
  - Commitment to confidentiality
  - Compliance with laws and policies
  - Incident reporting
  - Reimbursement

Logistics

- Three main options for binding a vendor to confidentiality requirements:
  - Compliance addendum;
  - Traditional NDA or confidentiality agreement; and/or
  - Preparing standard, organization-approved language to insert into services or other agreements.
- Many organizations have developed all three and use them in different situations.
  - Consider a confidentiality tool to guide business owners regarding when to use which form/language.
- Don't limit yourself to privacy and security – for example, the compliance addendum is a great opportunity to address other pertinent issues such as exclusions or Medicare access to records.

Confidentiality

- HIPAA: Acknowledge that vendor is not a business associate and require vendor to enter into BAA should scope of services change or HIPAA changes such that the vendor would be considered a business associate.
- Data Use Requirements:
  - Prohibit requesting or accessing data outside the scope of the engagement.
  - Maintain information obtained through "incidental" use or disclosure in strict confidence.
  - Do not use or disclose PHI for any purpose except to the extent incidental use or disclosure of PHI is necessary in performance of the services.
  - Do not maintain, copy or misappropriate any PHI.

Compliance

- Require vendor to comply with all applicable law, including state data privacy and security laws.
- Require vendor to comply with all organizational policies and procedures regarding access to information systems or premises, including:
  - User authentication;
  - Sharing of passwords;
  - Visitor sign-in/out and badge requirements; and
  - Remaining accompanied by organization personnel while on-site.

Polling Question #3

Incident Reporting

- Require vendors to report data security incidents in a manner similar to the breach reporting obligations required by HIPAA and state law.
  - A data security incident may be defined as any use or disclosure of confidential information in violation of the confidentiality agreement.
- Key Requirements for Vendor:
  - report the incident;
  - safeguard the confidentiality of the information involved in the incident;
  - take reasonable steps to destroy or return the information involved in the incident; and
  - take reasonable steps to mitigate any harm from the incident.

Reimbursement and Liability

- Particularly if a large amount of data is involved, or the potential exists for access to medical records or other sensitive information, consider:
  - Incident Reimbursement: Require vendor to reimburse organization for any costs, fines, penalties or expenses incurred as a result of the incident. Consider specifying which costs (if not all), cap on liability (tied to insurance?), insurance mandate, and exceptions to reimbursement (vendor not solely to blame?).
  - Indemnification: Vendor holds organization harmless and makes organization whole in the event of a claim arising from the vendor's use or disclosure of data.
    - More important in light of growing negligence claim activity.

Questions?

Biography & Contact Information

William Roberts is an associate in Shipman & Goodwin LLP's Health Law Practice Group and is the Chair of the firm's Privacy and Data Protection Group. Bill focuses his practice on health care corporate, regulatory, data privacy and compliance matters. He represents hospitals and health systems; academic medical centers; physician group practices; health insurance companies; behavioral health providers; federally qualified health centers; medical device and pharmaceutical companies and a variety of other public and private sector clients.

As Chair of the firm's Privacy and Data Protection Group, Bill routinely advises clients on data privacy and security laws, particularly as those laws intersect with the health care industry. He prepares comprehensive privacy and data security programs and policies for businesses, and regularly counsels clients regarding the collection, use, retention, disclosure, transfer and disposal of protected health information and personal information. Bill has assisted clients navigate and remediate over 150 data breaches.

William J. Roberts, Esq.
Shipman & Goodwin LLP
860-251-5051
wroberts@goodwin.com
http://shipmangoodwin.com/wroberts