Business Associates: How to Differentiate Your Organization Using HIPAA Compliance

December 2, 2015

William J. Roberts, Esq.

Forward Thinking Healthcare Solutions
It's What We Do

Today's Agenda

1. Who are HIPAA business associates?
2. How can I use HIPAA compliance to my advantage?
3. What must I do to comply with HIPAA?

About HIPAA

- HIPAA is a federal law that governs the use, disclosure and safeguarding of individually identifiable health information.
  - Referred to as "protected health information" or "PHI."
- 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.

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.

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 (but not PHI).
  - 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.

HIPAA Compliance is Good for Business (Seriously)

- View HIPAA compliance as less of a burden, and more of a marketing opportunity.
- Use compliance to differentiate yourself from the competition
  - HIPAA compliance statement on your website.
  - Post copy of HIPAA privacy policy?
  - Inform potential customers of highlights of your HIPAA compliance program – work with counsel, training programs, policies, risk assessments.
  - Address your commitment to compliance in sales and marketing materials.

HIPAA Compliance is Good for Business (Seriously)

- Be able to answer vendor screening tools quickly, accurately and confidently.
  - More and more health care providers use such tools to "weed out" potential vendors who lack sufficient HIPAA compliance programs – be ready so you aren't one of the vendors cut.
- Offer potential health care sector clients the option to review your HIPAA compliance program, policies and procedures.
- Make your HIPAA privacy officer available for questions.

How To Comply With HIPAA – A Checklist

- ✓ Privacy Policies
- ✓ Security Policies
- ✓ Appoint Privacy and Security Officer
- ✓ Training
- ✓ Data Incident Response Plan

Privacy Policies

- Identifying HIPAA covered entity clients
  - BAA process
- Collection, access and use of health information
  - What information will you/must you collect? Minimum necessary?
  - How will you use and/or disclose it? Internally? To subcontractors?
- Designated Record Set policy; Accounting of Disclosures
- Appointment of Privacy Officer
- Training Policy
- Complaints
- Sanctions for violation of HIPAA compliance program

Security Policies

- Risk assessment, analysis and management policies
- Appoint security officer
- Auditing
- Data backup/storage
- Disaster recovery/emergency operations
- Workstation use (e.g. access, passwords, authentication)
- PHI disposal (paper and electronic)
- Media re-use
- Encryption
- Physical security (e.g. locks, office access, securing files)

Training

- Business associates must establish a training program to provide HIPAA education and security awareness to employees and applicable contractors.
  - Conduct training within 30 days of hire and at least annually thereafter.
  - Consider periodic emails/reminders, posters or other educational approaches.
  - Address HIPAA, security best practices and knowledge of entity HIPAA compliance program, such as how to report a data breach.
- Training may be held online; however, if done through an online program, provide an opportunity for employee questions.

Data Incident Response Plan

- Define what is meant by a data incident.
  - Go beyond HIPAA.
- Establish an internal reporting protocol.
- Consider convening a data incident response committee (IT, admin, C-Suite, Privacy/Security officers, HR, legal).
  - Consider the benefit of attorney-client privilege.
- Understand legal and contractual obligations to clients and affected individuals.
- Address insurance coverage up-front and notify insurance if necessary.

Keeping Your HIPAA Compliance Program Current

- HIPAA compliance is not a "one and done" process and requires a continual, periodic review and update of your policies and procedures.
- The government and your customers will expect you to review your HIPAA compliance program at least once per year and any time there is a significant change to your organization (e.g. new office, new computer system)
  - Consider having an outside party review your HIPAA compliance program – benefit to fresh eyes and an independent analysis brings more credibility.
  - Establish a relationship to enable you to learn of changes to HIPAA.

Additional Compliance Strategies

- Ask: Does my *entire* organization need to comply with HIPAA? If not, which departments? Which employees? Which subcontractors?
  - Cater your HIPAA compliance program to your covered functions/ personnel.
- Ask: Do we already address what is required by HIPAA through other policies or programs?
  - Don't re-invent the wheel.
  - Many companies have existing policies which can be re-cast for HIPAA purposes – saves time and money.
- Ask: Can we incorporate HIPAA into an existing compliance program?

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 health care providers; health insurers; medical device and pharmaceutical companies and a wide variety of technology, consulting and other entities which operate in the health care sector.

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

Compliance In 3 Steps!

THE GUARD

One simple cost effective solution for HIPAA, HITECH, Omnibus, GLB, and PCI compliance

✓ Award winning three-step proprietary methodology ✓ Dedicated Compliance Coach

ACHIEVE

Quickly and easily self-audit, identify deficiencies (Gaps), and correct the Gaps (Remediate)

✓ Built in Training, Policy & Procedure Templates ✓ Meaningful Use, Security Risk Assessment

ILLUSTRATE

Show Auditors, Covered Entities (CE), and Business Associates (BA) your total compliance plan

✓ Remediation Planning and Tracking

✓ Tracking and Attestation

MAINTAIN

Advanced task management of vendor, employee, Business Associates, training, and attestation

✓ Incident Management

✓ Document & Version Controls

HIPAA Education Series sponsored by: Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

www.compliancy-group.com

855.85 HIPAA (855.854.4722)