Managing Security: HIE and Business Associates

The Twentieth National HIPAA Summit

Phyllis A. Patrick, MBA, FACHE, CHC

Phyllis A. Patrick & Associates LLC

March 27, 2012

Topics

- The Business Associate's Role and Responsibilities under Healthcare Reform and HITECH
- Managing Relationships
  - Understanding and Evaluating the Risks
  - Expectations: What should Covered Entities expect from their Business Associates?
- Health Information Exchange: A New Critical Business Associate involved in Sharing of ePHI

Significance of HITECH

- Mandatory Federal Breach Reporting Requirements
- New Privacy Requirements (Privacy Rule Amended)
- Penalties
- **Business Associates – HIPAA coverage (Privacy and Security Rules) apply directly (02/2010)**

What is a Business Associate?

- "…. on behalf of a covered entity or an organized health care arrangement in which the covered entity participates…… **performs or assists in the performance of**

  (a) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

  (b) Any other function or activity regulated by this subchapter; or…

BA Definition (Cont'd)

- Provides…. Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity… **where provision of the services involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate** of such covered entity or arrangement…"
- A covered entity may be a business associate of another covered entity. (*45 CFR 160.103*)

Statutory Obligations of BAs

- **Administrative Safeguards** *(45 CFR 164.308)*
- **Physical Safeguards** *(45 CFT 164.310)*
- **Technical Safeguards** *(CFR 45 164.312)*
- **Policies and Procedures and Documentation Requirements** *(45 CFR 164.316)*
- Certain **Privacy Requirements**

✓ Penalties apply to BAs to same extent as for Covered Entities.

✓ Risk of significant civil fines and possible

Extension of HIPAA Privacy and Security to BAs

- BAs that obtain or create PHI pursuant to a written contract or arrangement are subject to privacy provisions that covered CEs must meet

(45 CFR 164.504(e) and 45 CFR 164.502(e))

Privacy Provisions

- BAs must comply with **disclosure of PHI** restrictions and standards, e.g.,
  - **Minimum Necessary**
  - **Limited Data Set**
  - **Accounting of Disclosures**
  - **Restrictions on Disclosures to Health Plans**
  - **Individual Access to PHI/Access Reporting**
  - Prohibition on **Sale of PHI**
  - **Marketing and Fundraising restrictions** (communications made on behalf of CE)

✓ **The BA acts on behalf of the CE.**

✓ **Individual may request accounting directly from BA.**

Breach Notification Requirements

- Involves PHI that has been **accessed, acquired**, and/or **disclosed**
- **Timelines** for reporting
- **Notification** to affected individuals, media, and HHS
- Investigation process, mitigation, and documentation
- Vendors of Personal Health Record (PHR) *(HITECH Section 13407)*

The CE/BA Relationship

- Understanding and Evaluating the Risks
- Managing the Relationship
- HIEs: A New Type of Business Associate

Understanding and Evaluating the Risks

- **Who** are your BAs?
  - Not all vendors are BAs.
  - Vendors that don't need access to PHI in order to provide services are not BAs.
- **How many BAs** do you have?
- How do you **document your BA relationships**?
  - Contract files
  - Automated tracking system
- How often do you **renew BA Agreements**?
- Who (which dept/area) is **responsible for managing the BA database**?

Understanding and Evaluating (Cont'd)

- Does your organization have **a vendor relations program**?
  - Who (which dept.) coordinates?
  - How does the vendor program interface with the BA program?
  - How do vendor management policies affect the BA program and relationships with BAs?
  - Do you have an automated program for managing vendors?
- Key issues: vendor sanctions and exclusions checking, conflict of interest policies, oversight of vendors

Understanding and Evaluating (Cont'd)

- ✓ Have you prioritized your BAs based **on risk to your privacy and security programs?**
  - Higher risk vendors may include IT vendors, EHR vendors, billing companies, medical transcription companies, record storage companies (e-storage and paper storage), contract coders, collection agencies, release of information vendors, etc.
  - Do you conduct audits of high-risk vendors?
- ✓ Do you require high-risk vendors to

Understanding and Evaluating (Cont'd)

- How are **department heads and vendor champions/liaisons** involved in the relationship?
  - Do they advise business associates on their responsibilities?
  - Do they assist in monitoring business associates for compliance with the organization's privacy and security programs?
- Have you educated dept. heads and liaisons regarding their roles and responsibilities for protecting privacy and security of confidential information?

Managing the Relationships

- Regulatory requirements
- New responsibilities and expectations
- Contractual obligations

Managing the Relationships

- Are your business associates aware of the HITECH changes and their new and expanded responsibilities for protecting your organization's PHI?
- Have breach notification responsibilities and accountabilities been clearly defined – both for the covered entity and the business associate?
- How will you support each other in the event of a breach?
- Who is responsible for financial outlays associated with breach mitigation?

Managing the Relationships (Cont'd)

- Have you modified your contract and BA Agreement to reflect changes in requirements and your expectations of your BAs?
- How often do you communicate with your business associates regarding your expectations for safeguarding your confidential information?

Enforcement Changes & Trends

- **"Business Associates Beware: First HIPAA Enforcement Action Against a Business Associate (And the Plot Thickens with Transparency Demands)"**
- *Minnesota Attorney General brings first formal enforcement action against a business associate, Accretive Health, Inc. for alleged HIPAA violation.*
- Security Allegations
- Deceptive Practice Allegations

Adam H. Greene and Rebecca L. Williams (12.06.12)

Security Risk Assessment for the Business Associate

- Can you demonstrate compliance with the HIPAA Security Rule evaluation standard?
- Can you demonstrate that your policies, procedures, and practices are up to date and that the review and approval processes are documented?
- Do you have a risk mitigation planning process, i.e., how have you mitigated risks found in previous risk assessments?

HIEs: New Relationships

- HITECH Act authorized ONC to award grants to states to build Health Information Exchange (HIE) capacity to improve quality and efficiency of care.
- Funding for development of “necessary governance, policies, technical services, business operations and financing mechanisms for HIE.”

A different type of BA

- Many parties are involved in HIEs
  - Development and maintenance phases
  - Governance and Community issues
  - HIE “sponsor”, vendor(s), third party contractors
  - Multitude of “Participants” – health systems, hospitals, physicians (large and small practices), allied health providers, laboratories, imaging centers, pharmacies, payers, etc.) – potential for 100’s of organizations and entities

Other Issues related to HIEs

- Access can be problematic – many users, user access and authentication issues
- Role of the Payer – now and in the future
- Technical Issues -- infrastructure and processes, system customization , technical capabilities, resources
- Due diligence Issues --- technology vendors and sub-contractors
- Role of HIE Workforce Members

Other Issues (Cont'd)

- Interstate jurisdiction and related issues
- Consenting Process
- Patient Access and Role of the Patient – PHR scenarios
- Implementation of Privacy enhancements to HITECH, e.g.,
  - If payers are participants in the HIE, how to implement patient request for restrictions on access when payment is made in full
  - How to provide Patient access to electronic records

Will HIEs become a new category?

- The HIE is both a Business Associate to the HIE Participants and also works with many different types of Business Associates.
- Future Role?

Privacy and Security Compliance in HIE: Key Factors

- HIE/RHIO as Business Associate
- Information in the public domain
- Policies and procedures
- Breach Response, Notification, Reporting
- Compliance with State laws
- Patient Consent
- User Authorization and Management

connects to everything else.”

Leonardo da Vinci

PHYLLIS PATRICK + Associates

Culture | Security | Privacy

Phyllis A. Patrick, MBA, FACHE, CHC

Phyllis A. Patrick & Associates LLC

www.phyllispatrick.com

phyllis@phyllispatrick.com

914-696-3622