A MILLIMAN GLOBAL FIRM

Milliman USA

Consultants and Actuaries

The IT Vendor: *HIPAA Security Savior for Smaller Health Plans?*

Agenda

- Definitions
- Problem
- Expectations
- Responsibilities by specification
- Collaboration Benefits
- Implementation process

Vendor Defined

- Benefits System vendor
- TPA

Smaller Health plan defined

- Self-insured with 100 to 100,000 participants
- Activities
  - Enrollment
  - PHI management
  - Claims
  - Miscellaneous other
- Often single employer or multi-employer plans

Flexibility in Rule

Covered entities may use any security measures that allow the covered entity to **reasonably and appropriately** implement the standards and implementation specifications

-- §164.306 (b)(1)

Problem: Issue I

What measures are:

“Reasonable and Appropriate”?

Problem: Issue II

Are the costs of determining "*reasonable and appropriate,*" *measures*

reasonable and appropriate?

Problem: Issue III

HIPAA requires **Actions** and **Documentation**

Problem: Health Plan Perspective

- Limited internal capabilities
- Consultants too expensive
- Boilerplates general and open-ended
- Vendor dependency for IT
- Document, document, document
- Who cares?

Problem: Vendor Perspective

- Not the covered entity
- Assume compliance
- Other client service priorities
- Who pays?
- Who cares?

Expectations

- Health plan: vendor has solved this
- Vendor: health plan is the covered entity
- Both: little chance of enforcement

Single Systems According to NIST

- Be under the same direct management control
- Have the same function or mission objective
- Have essentially the same operating characteristics and security needs
- Reside in the same general operating environment

Opportunity

- Overlapping features among installations and similar clients
- Half of requirements technical
- Vendor natural focus for plans
- Documentation similar among installations

Shortcoming of Collaborative approach

- Management control divided between vendor and healthplan
- Installation specific issues
- Coordination of implementation process
- Responsibility = liability?
- Still not resource free

Responsibility by Specification

- Administrative (shared)
- Physical (primarily healthplan)
- Technical (primarily vendor)

Administrative Safeguards

- Security management process (V/HP)
- Assigned security responsibility (HP)
- Information access management (V/HP)
- Training (HP)
- Incident procedures (V/HP)
- Contingency plan (V/HP)
- Evaluation (V/HP)
- Business associate contracts (HP)

Physical Safeguards

- Facility access controls (HP)
- Workstation use and security (HP)
- Device and media controls

  (HP primarily—vendor may provide DB backup)

Technical Safeguards

- Access controls (V)
- Audit controls (V)
- Data integrity (V)
- Entity authentication (V)
- Transmission security (V)

Example:

Risk Assessment

- Exceeds technical capabilities of smaller healthplans
- Much of assessment similar for comparable plans with same system

Example:

Risk Assessment: Components

1. EPHI boundary definition
2. Threat identification
3. Vulnerability identification
4. Security control analysis
5. Risk likelihood determination
6. Impact analysis
7. Risk determination
8. Security control recommendations

Example:
Assigned responsibility

Boilerplate job description can be edited by each healthplan

Example:

Security Management Process

- Risk analysis focuses on vendor system
- Risk management focuses on vendor system
- Healthplan determines sanction policy
- Vendor provides tool or performs system activity review

Example:

Security Awareness and Training

- Vendor could provide:
  - Security reminders
  - Protection from malicious software
  - Log-in monitoring
  - Password management controls
- Training program options

Example:

Device and Media Controls

- Disposal and media reuse; accountability systems
  - Vendor provides proposed guidelines to clients
  - Clients edit and implementation guidelines
- Data backup and storage: Vendor may propose Internet and ASP options

Example:

Access Controls

- Vendor system includes:
  - Unique User Identification
  - Emergency Access Procedure
  - Automatic Logoff
  - Encryption and Decryption

Collaboration Benefits: Vendor

- Leadership
- Value added service to client
- Controlling healthplan consultants
- Resolution of system security issues
- Improved market positioning

New vendor opportunities

- Secure backup services
- Installation specific assistance
- Intrusion detection services
- Secure messaging and encryption
- Ongoing security management

Collaboration Benefits: Health Plan

- Spreading costs
- Managing HIPAA realistically
- Synergies

Vendor Implementation Options

- Serial Approach: Implement internal solution then involve clients
- Group solutions
  - User groups
  - Target clients
  - Workshops

Stumbling Blocks

- Variations on installs
- Health plan specific issues
- Coordination
- Vendor apathy
- Resources

Implementation Process

- Vendor acceptance
- Determine strategy
- Assess resource needs
- Evaluate vendor system
- Modify system as needed
- Prepare template policies
- Implement policies at installations

Strategic issues

- Healthplan or vendor centered approach
- Security program structure
- Implementation sequence
- Cost structure
- Kick-off

Next Steps: Vendor

- Conduct preliminary system assessment
- Develop client participation strategy
- Develop cost strategy
- Prepare boilerplate materials
- Communicate program

Next Steps: Healthplan

- Develop proposal
- Approach vendor
- Approach other vendor users

A MILLIMAN GLOBAL FIRM

Milliman USA

Consultants and Actuaries

The IT Vendor?

Questions?

A MILLIMAN GLOBAL FIRM

Milliman USA

Consultants and Actuaries

John L. Phelan, Ph.D.
Health Management
and Technology Consultant
Telephone: 818/707-7818
E-mail: john.phelan@milliman.com