Lessons Learned from the GNYHA HIPAA Security Consortium

Susan Stuard, Greater New York Hospital Association
Brian M. Wyatt, Ropes & Gray LLP

Presentation Overview

1. Process lessons learned
   – Review of HIPAA Security Consortium project and lessons learned about the project's structure
2. Subject-matter lessons learned
   – Discussion of HIPAA Security compliance issues raised during work on HIPAA Security Consortium or through discussion of HIPAA Security Workgroup

Lessons Learned: HIPAA Security Consortium Process

Greater New York Hospital Association (GNYHA)

- A trade association representing more than 250 not-for-profit hospitals and continuing care facilities
- Members located in New York City metropolitan area and throughout New York State, as well as in New Jersey, Connecticut, and Rhode Island

Background - Privacy

- Approach to Security Rule premised on experience with Privacy Rule
- Formed a HIPAA Privacy workgroup
  - Met monthly between Jan 2002 and July 2003
  - Forum to discuss interpretation of regulation and implementation concerns
  - Privacy officers, in-house counsel, HIPAA project managers, medical records, etc.
  - Now meets bi-monthly – still a great need to discuss compliance issues and benchmark practices

Background - Privacy

- Formed HIPAA Privacy Consortium
- Hired law firm of Ropes & Gray to:
  - Undertake a preemption analysis
  - Develop 28 policies and documents needed to comply with Privacy Rule and to account for preemption issues (BAA, Notice of Privacy Practices, authorization, etc.)
- Benefits:
  - Share the legal costs among the participants
  - Joint interpretation of the regulations – safety in numbers!
  - More than 120 institutions participated

HIPAA Security Workgroup

- Formed HIPAA Security Workgroup
  - Started meeting monthly in November 2003
  - Comprised of Security Officers, Privacy Officers, network security and IT staff, HIPAA project managers, internal audit staff, etc.
  - Conversations are not technical in nature but, rather, focus on benchmarking compliance approaches
  - Group has just become comfortable with one another and we expect to cover a lot of ground this fall

Security Consortium

- Based upon success of Privacy Consortium, members requested that GNYHA pursue a HIPAA Security consortium concept
  - Concern about vagueness of Security Rule, members looking for safe haven of joint interpretation
  - Same financial model, share costs of professional services
- Determined that we could undertake the following as a group:
  - Risk assessment/gap analysis tool
  - Set of security policies and procedures
  - An all-day training session

Vendor Selection Process

- GNYHA issued an RPF and responses were evaluated by members
- Held a vendor presentation session for finalists to present and members evaluated finalists
- Members chose:
  - Security consulting firm, International Network Services
  - Law firm, Ropes & Gray
- Ultimately, more than 100 hospitals and long-term care facilities participated

Scope of Work

- Risk assessment tool migrated to gap analysis scorecard tool
  - Caused consternation among some participants
  - Consultants felt gap analysis model was what they could reasonably accomplish for a large, diverse group
- Policies and guidance documents
  - Created a model policy or guidance document for all 36 implementation specifications
  - Designed to be collapsed and/or integrated with current policies
  - Consistent with documents prepared for HIPAA Privacy Consortium

Scope of Work

- GNYHA's caveats at start of project:
  - Products will only start compliance process
  - Institution-specific remediation advice is not part of scope
- Conducted reference-site visits to assess current security at small, medium and large institutions
- Issued draft products for comment at two points during process
  - Participants were not as active as we had hoped in the commenting process

Lessons Learned from Consortia

- Tremendous financial benefits of sharing costs
- Great benefits to joint interpretation
- Most effective for a select type of work
    - Policies and procedures are best fit
    - Legal interpretation that cuts across organizations will also work well
    - Technical or institution-specific issues are not easily addressed

Lessons Learned from Consortia

- Be prepared for the success rate
  - 80% will find Consortium products very beneficial
  - 20% will not be as pleased
- Participants get out what they put in
  - Critical that participants have an opportunity to review draft documents, and make sure that they do
  - Tools are a starting point – participants must deploy and customize them for own institution
- Need to over-communicate and belabor any changes to scope of work

Lessons Learned from Consortia

- Consortia can offer some hard and firm advice, but majority of work can only offer a guideline
  - Narrows scope of compliance decisions, but still must make decisions about what is best for your institution
- Keep forum active after project winds up
  - Used HIPAA Security Workgroup to keep discussion going

Lessons Learned: Security Compliance Issues

Security Compliance Issues

- Process Issues
- Legal Issues
- Specific Compliance Issues

Security Compliance Issues

- Process Issues
  - Governance
  - Risk Analysis Methodology
  - Addressable Implementation Specifications

Process Issues: Governance

- Who is responsible for leading the HIPAA Security compliance effort?
  - Overwhelmingly responsibility has been handed to IT staff
  - What about legal, compliance, internal audit, clinical engineering?
  - Strong concern that legal and compliance do not understand that security compliance is documentation intensive

Process Issues: Risk Analysis Methodology

- Risk analysis is required, and the fundamental element that informs the compliance effort
- How to do this???
  - Recent draft WEDI White Paper
  - 8/12/04 CMS FAQ (Answer #3228)
  - Commercially available tools?
- Covered entities have strong concerns about this process

Process Issues: Addressable Implementation Specifications

- "Addressable" does not mean "optional"
  - Must still satisfy the applicable standard
- Cannot just decide not to implement an AIS – have to follow the mandated steps
  - See Handout
  - Also discussed in several of the CMS FAQs released on 8/12/04
- Big task because, 21 of 34 implementation specifications are addressable implementation specifications (AISs)
- Reality: A given covered entity is unlikely to implement all of them

Process Issues: Addressable Implementation Specifications

- Authorization and/or Supervision
- Workforce Clearance Procedure
- Termination Procedures
- Access Authorization
- Access Establishment and Modification
- Security Reminders
- Protection From Malicious Software
- Log-in Monitoring
- Password Management
- Testing and Revision Procedure
- Applications and Data Criticality Analysis
- Contingency Operations
- Facility Security Plans
- Access Control and Validation Procedures
- Maintenance Records
- Accountability
- Data Backup and Storage
- Automatic Logoff
- Encryption and Decryption
- Integrity Controls
- Encryption

Process Issues: Addressable Implementation Specifications

- For each AIS, the covered entity must first determine whether it is a reasonable and appropriate security measure to apply to its particular security framework
- This analysis should take into account the following factors:
  - Size, complexity and capabilities of the covered entity
  - Covered entity's technical infrastructure, hardware and software security capabilities
  - Cost of implementation
  - Probability and criticality of potential risks to EPHI
  - Results of covered entity' risk analysis
  - Covered entity's risk mitigation strategy
  - Security measures already in place at the covered entity
- What's not on this list???

Process Issues: Addressable Implementation Specifications

- Based on the outcome of this decision, the covered entity has three “options” for compliance:
  - Option One: If an AIS is determined to be reasonable and appropriate, the covered entity must implement it
    - In this circumstance, the AIS is mandatory and should be treated like a required implementation specification

Process Issues: Addressable Implementation Specifications

- Option Two: If an AIS is determined not to be reasonable and appropriate, based on the factors noted above, then the covered entity must take the following actions:
  - Document why it would not be reasonable and appropriate to implement the implementation specification and the rationale behind that decision;
  - Determine whether there is an equivalent alternative measure that would be reasonable and appropriate to implement that accomplishes the same end as the AIS; and
  - Implement any such reasonable and appropriate equivalent alternative measure

Process Issues: Addressable Implementation Specifications

- What is an “equivalent alternative measure”?
  - Not defined in the HIPAA Security Regulations
  - Any measure that allows the covered entity to comply with the standard by satisfying the same end as the AIS
    - A technical safeguard, a physical safeguard, or an administrative safeguard
  - An Example (from HHS):
    - “For example, the addressable implementation specification for the integrity standard calls for electronic mechanisms to corroborate that data have not been altered or destroyed in an unauthorized manner (see 45 CFR 164.312 (c)(2)). In a small provider's office environment, it might well be unreasonable and inappropriate to make electronic copies of the data in question. Rather, it might be more practical, affordable and serve as a sufficient safeguard to make paper copies of the data.”

Process Issues: Addressable Implementation Specifications

- Option Three: Where you determine that (1) an AIS is not reasonable and appropriate your its situation, (2) there is no reasonable and appropriate equivalent alternative measure, and (3) the standard can be met without implementation of the specification or an alternative
- In this scenario, you must document:
  - The decision not to implement the AIS (either as specified or by an equivalent alternative measure);
  - The rationale behind that decision; and
  - How the underlying standard is being met

Process Issues: Addressable Implementation Specifications

- How often will you end up at "option" 3?
- Another example from HHS to illustrate:
  - "For example, under the information access management standard, an access establishment and modification implementation specification reads: "implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process" (45 CFR 164.308(a)(4)(ii)(c)). It is possible that a small practice, with one or more individuals equally responsible for establishing and maintaining all automated patient records, will not need to establish policies and procedures for granting access to that electronic protected health information because the access rights are equal for all of the individuals."

Security Compliance Issues

- Legal Issues
  - Documentation
  - Involving Counsel/Privilege
  - Interface with HIPAA Privacy

Legal Issues: Documentation

- Goes beyond HIPAA Privacy Regulations' documentation requirements
  - Not only retention (for 6 years)
  - Not only policies and procedures, and other required documents like NPPs
- Long list of "action, activity or assessment" items that must be documented
  - See Handout
- Think about who needs to be involved in this

Legal Issues: Documentation

- Not just documenting but:
  - Availability: "Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains."
  - Updating: "Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information."

Legal Issues: Involving Counsel/ Privilege

- Remember that your risk analysis and other documentation will evidence existing vulnerabilities
  - Consider how results of your risk analysis will be used and distributed in your organization
  - Consider how (and by whom) documentation regarding AISs will be created and maintained
- Suggestions to consider:
  - Involve legal counsel early and often
  - Limit distribution of risk analysis, and do not distribute it electronically
  - Engage outside consultants through legal counsel

Legal Issues: Interface with HIPAA Privacy

- Keep in mind HIPAA Privacy
  - Reasonable safeguards requirement (a/k/a the "Mini Security Rule")
  - Minimum necessary rule
  - Training
- But some key differences:
  - Electronic PHI vs. PHI
  - No OHCA concept in Security (though ACE and hybrid entity concepts carry through)
  - No permitted incidental uses and disclosures under Security
  - "Evaluation" and review and updating of documentation required

Legal Issues: Interface with HIPAA Privacy

- Electronic PHI – PHI transmitted or maintained on electronic media:
  - Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card
  - Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media.
  - Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission
- Don't forget about medical devices and equipment

Legal Issues: Interface with HIPAA Privacy

- Privacy and security violations often go hand-in-hand
- OCR and CMS will be talking to each other
  - So a complaint to one may well trigger an investigation by the other

Security Compliance Issues

- Specific Compliance Issues
  - Auditing Requirements
  - Facility Access Controls
  - Incidental Disclosures
  - Workstation Definition
  - Biomedical Devices

Specific Compliance Issues: Auditing Requirements

Administrative Safeguards

- Information System Activity Review (required IS) §164.308(a)(1)(D)
  - under Security Management Process standard
- Log-in Monitoring (AIS) §164.308(a)(5)(C)
  - under Security Awareness & Training standard
- Evaluation (standard – required) §164.308(a)(8)

Technical Safeguards

- Audit Controls (standard – required) §164.312(b)

Specific Compliance Issues: Auditing Requirements

- NIST 800-66 – Draft Resource Guide for Implementing HIPAA Security Rule
- 5 activities for Audit Controls (§164.312(b)):
  1. Determine systems or activities to be tracked or audited
  2. Select the tools that will be deployed for auditing and system activity reviews
  3. Develop and deploy the Information System Activity Review and Audit Policy
  4. Develop appropriate standard operating procedures
  5. Implement the audit/system activity review process

Specific Compliance Issues: Auditing Requirements

- Review Considerations
  - Who will review these logs and events?
  - Organization structure needs to be considered
  - Are there periodic reviews, and if so, what is the frequency?
  - Is there an ability to go back and review and event from a previous month or period?
  - Are logs and audit trails preserved in such a way that they can not be altered?
  - Considerations needed for appropriate reviews of logs – system administrators should not be self-policing
  - Are events reviewed on a pro-active or reactive basis?
  - Do logs reflect only user activity or administrator activity as well?

Specific Compliance Issues: Auditing Requirements

- Legal & Risk Management Issues
  - What about the collection of logs that no one reviews? What happens if an incident occurs that could have been prevented?
  - What happens when logs are reviewed and there were indications of problems that no one sees or investigates?
  - What are the reporting mechanisms when a discovery is found? Who gets involved? Is there a formal incident response plan, disciplinary action policy, etc.?

Specific Compliance Issues: Facility Access Controls

- Hospitals and LTC facilities are inherently public institutions
- Patient safety and public access are not noted as factors to weigh against physical security
- How will CMS view it if hospitals and LTC facilities provide stronger facility access controls for network closets and server rooms than outpatient clinic reception or nurses stations?

Specific Compliance Issues: Incidental Disclosures

- Incidental Disclosures
  - No provision in Security Regulations (unlike Privacy)
  - Will reasonable measures be deemed adequate?
  - Hard to balance reading of strong language (ensure, etc.) with scalability and reasonableness language

Specific Compliance Issues: Workstation Definition

- Definition is very broad
  - Includes “electronic media stored in [an electronic computing device’s] immediate environment”
- When does EPHI on electronic media become part of a “workstation”?
  - e.g., flash memory
- Important because of standards that specifically reference “workstations”
  - e.g., Workstation Use (§ 164.310(b)) and Workstation Security (§ 164.310(c))

Specific Compliance Issues: Biomedical Devices

- FDA issue
- Some biomedical device manufacturers are citing FDA policy as a reason they cannot install basic security patches on networking software
  - Manufacturers tell hospital that they can't install security patches "because of FDA rules"
- Recent article in *Network World* documents that hospitals are starting to patch over objections and threats of vendors

- Susan Stuard
  GNYHA
  stuard@gnyha.org

- Brian M. Wyatt
  Ropes & Gray LLP
  bwyatt@ropesgray.com

Boston
New York
San Francisco
Washington, DC