Advanced Issues in HIPAA Privacy

HIPAA Summit West II

San Francisco, California
March 15, 2002

Michael Calhoun
Principal, Healthcare Consulting
One Embarcadero, Suite 2800
San Francisco, California
415.439.2600, mcalhoun@csc.com

Contents

- **Common Themes from Privacy Assessments**
- **Complex Privacy Issues**
- **Issue Drill Down**
- **Potential Changes in the Privacy Rule**

Introduction

After the intensity and resource drain of the gap assessment and making sense of the scores of exposure points that result comes the hard part: Remediation.

The temptation is to default to an approach that takes on the gaps in a linear sequence driven by real and immediate limitations on management, labor force, and financial resources.

The ideal is to think critically about compliance gaps, remediation requirements, and business needs then fashion an approach that achieves compliance with minimal business process disruption and possibly some performance improvement.

The challenge is to keep it simple.

Privacy Assessment and Remediation Planning Recurring Themes

1. Strategic decisions on the level of PHI protection are needed for Business Associate (BA) and Covered Entity (CE) roles.

- HIPAA reaches BAs through terms in the BA contract. CEs and BAs typically have numerous relationships that will require BA contracts

→

- As a BA, how to meet differing contract requirements from numerous CEs?
- As a BA, implementing some contract terms may be similar to CE requirements
- As a CE, how to standardize BA contract terms?

2. Operationalizing "minimum necessary" standards and "inappropriate use" reporting often requires redesign of data access rights and strong role definitions.

→

What is the best approach for meeting the requirement to limit PHI to that which is minimally necessary for the intended purpose while not disrupting business process, requiring deep resource investment, and or becoming big brother?

3. The design for any new space should maximize the contribution of physical layout and support facilities to meeting privacy and physical security requirements.

- Both Privacy and Security are implicated
- Privacy concerns ***who*** gets what information, Security concerns ***how*** the information is protected

→

- Retro fitting is expensive. Insightful planning offers significant economy in achieving privacy/physical security mandates
- Segregate work space by roles and PHI?
- What to do about fax machines, copiers, and printers?
- How to protect computer screens, manage telephone conversations?

4. Self-insured health plans should meet HIPAA privacy requirements regulations.

- Employers are not covered by HIPAA, but under certain circumstances the self-insured plan is.

→

Currently, plan management follows confidentiality principles, but few have written policies and procedures, even fewer have HIPAA mandated protections

Privacy Assessment and Remediation Planning Recurring Themes

5. Call Center practices and caller verification standards frequently require re-design.
- Both Privacy and Security are implicated.

→
- Verification of individuals and others receiving PHI typically is not sufficiently rigorous.
- Call centers accessing PHI need to be isolated from other work areas.

6. Policy and procedure content and documentation are frequently non-existent or do not meet the specifics of HIPAA mandates.
- Documentation is a cornerstone of HIPAA Privacy and will be the first point of contact for audits/enforcement

→
- Most organizations have confidentiality policies, many enforce confidentiality practices. Few come close to what HIPAA requires in content and documentation
- Very few organizations document the PHI they have and all the places it resides.

7. A robust Project Management Office is needed to assure the coordinated development of common policies and procedures and oversee entity implementation across the organization and all three HIPAA remediation areas.

→
- The scale and intensity of privacy remediation will require full time engagement (internal or external) and numerous resources from across the organization over an extended time
- There are efficiencies to be captured through coordination with TCS and Security efforts

8. A central privacy infrastructure is needed to assure the greatest economy of resources in achieving a uniform level of compliance across the organization.
- For most organizations, just

→
- For most organizations, having just a Privacy Official is not enough
- Centralizing the oversight of privacy requirements is advisable, including the individual's access to review, copy, and amend PHI; informing about disclosures;oversight of minimum necessary requirements and physical safeguards

Contents

- Common Themes from Privacy Assessments
- Complex Privacy Issues
- Issue Drill Down
- Potential Changes in the Privacy Rule

Identification and Verification for Communication of PHI

- **Under various provisions, e.g. consent, authorization, minimum necessary, disclosure of information, HIPAA requires that only those permitted can receive PHI.**
- **A big exposure for most entities is the overlap between Privacy and Security requirements: *How does the organization assure that PHI being communicated is actually being received by the intended recipient?***
  - ***Internal e-mail challenges*:**
    - > Right address, anyone has access – need safeguards
    - > Right person, too much information -- no more data dumps!
  - ***External e-mail challenges*: Right address -- but who is on the other end, or is that your problem?**
  - ***Phone*: How do you really know who is on the other end -- is date of birth and mother's maiden name really enough?**
  - ***Paper*:**
    - > How do you know the addressee is the one receiving the document?
    - > Who is reading the faxes—incoming? outgoing?
    - > Where is the printer and who has access?

Self-insured health plans

- **A potential sleeper!**
- **Employer self-insured health plans act as small health plans or insurers regarding the creation and communication of PHI. HIPAA Privacy probably applies unless no PHI is ever available to the employer (or an employee supporting the plan)**
- ***Is the plan self-managed or outsourced?*** There is a HIPAA exemption if
  - Health benefits are available solely through a contract with an insurance issuer or HMO
  - The plan does not create or receive protected health information, except for summary health information
- ***What PHI is available on site?*** Even for outsourced plans, what information is obtained for oversight, quality control, employee appeals of coverage denial?
- ***What are the protections?*** – physical space, IT?
- ***What is management's access?*** Is PHI available for sick leave enforcement; preventive healthcare program referrals; drug testing; annual reviews/promotion? Did you get consents?
- **Sources**
  - § 160.103 Definitions
  - § 164.501 Definitions
  - § 164.502 (e)(1) Uses and disclosures of PHI: Standard: disclosures to business associates.
  - § 164.504 Uses and disclosures: organizational requirements.
  - §164.504 (f) Requirements for group health plans
  - §164.510 Uses and disclosures for which an authorization is required
  - §164.510 (b) (2) Uses and disclosures with the individual present
  - § 164.514 (d) Minimum Necessary Requirements
  - § 164.520 (a) Notice of privacy practices for protected health information
  - § 164.530 (k) Administrative Requirements – group health plans

Recurring Complex Remediation Challenges

- **Pre-emption of state law**
  - **There is a separate session on this question. It is mentioned here to emphasize its importance and its complexity**
  - **Privacy provisions for Covered Entities preempt state law except–**
    - > If the Secretary determines that the state law preempts HIPAA
    - > The state law relates to the privacy of health information and is more stringent
    - > The state law provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention
    - > The state law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals
  - ***Key issue* : What is "more stringent"? Who decides? What's the risk?**

Transitions Rules – Preserving Access to Pre-HIPAA PHI

- **Under HIPAA, any use or disclosure of PHI requires consent , authorization, or regulatory permission including PHI in a CE's possession on the effective date.**
- **There are, however, specific "transition" rules governing how PHI collected before the effective date can continue to be used after the effective date without having to meet the consent and authorization requirements.** (§ 164.532 Transition provisions)
  - The CE must have a consent, authorization, or other express legal permission to use or disclose PHI before the April 14, 2003 date for PTO or other activities and must comply with those terms after April 14
- **Most provider organizations collect consents, but for use of PHI or for procedures?**
- **Most payer organizations collect permission to disclose, but what about internal use?**
- **What is the potential impact on the organization? How rapidly do patients/customers turnover?**
- **What is the best approach to address the problem?**
  - Start now to obtain proper permissions, on a going forward basis
  - Updating permissions for archived, inactive, infrequent patients/customers. How?

Training

- **HIPAA has similar training requirements for both Privacy and Security.**
  - Initial training by the effective date: Privacy -- April 14, 2003; Security – not set
  - Privacy/Security
    - > Each new employee
    - > With each change in HIPAA privacy rules, company privacy Policies and Procedures
  - Security annual self-certification
- **Training should be on policies and procedures and must be documented**
- **How do you train everyone and document it appropriately cheaply and effectively? Can HIPAA training be integrated into an overall company training infrastructure?**
  - > Using the existing training infrastructure (e.g. Corporate's new employee training
  - > Company-wide or by entity, department?
  - > Who?/How? (e.g. Privacy Officer: content; Corporate training: process)
  - > Outsource training to web-based vendors/systems
- **Potential Resources**
  - **Quick Compliance** -- www.quick compliance.com
  - **Celexx** -- www.celexx.com/home/home.html
  - **Easyi** -- www.easyi.com/topics/hipaa.asp
  - **CMHC Systems** -- www.cmhcsystems.com
  - **Convansys** -- www.convansys.com
  - **Extreme Solutions** – www.exstreamsolutions.com/hipaa.asp
  - **HIMSS** –www.himss.org

Contents

- Common Themes from Privacy Assessments
- Complex Privacy Issues
- Issue Drill Down
- Potential Changes in the Privacy Rule

Minimum Necessary Requirements -- Overview

- **Basic Rule:** When a CE uses (internally), discloses (to external recipients), and requests protected health information (PHI) it must make "reasonable efforts" to ***limit the PHI to that which is minimally necessary*** for the intended purpose and that it link employee access by duties/role to specific categories of PHI.
- **Implementation requirements:**
  - For ***uses*** of PHI, a CE must identify—
    - > Persons and classes of persons in the workforce who need access and limit their access to the categories of PHI as described below
    - > For each person or class of person, the category or categories of PHI to which access is needed and appropriate conditions
    - > Make reasonable efforts to limit access consistent with these classes and categories
  - For ***routine disclosures*** of PHI, a CE must implement policies and procedures that limit the PHI disclosed to the amount necessary
  - For ***other disclosures***, a CE must—
    - > Develop criteria for limiting the PHI disclosed to minimum necessary
    - > Review requests for disclosures on an individual basis consistent with this criteria
  - For ***requests*** for PHI, a CE must limit any request for PHI to that necessary to accomplish the intended purpose
  - **A CE must reasonably ensure that these requirements are met**

Minimum Necessary Requirements – Key Issues

- **Managing minimum necessary for internal use:**
  - **How to implement the linkage of classes of employees and categories of PHI?**
    - > Differing approaches for large/complex organization vs. small
    - > The impact of standard practice in the community and how it evolves
    - > The impact of cross-training employees for multiple functions
    - > Ongoing oversight/management of access rights
  - **Is managing access rights enough?**
    - > The rule is to limit the information not just an employee's access to it
    - > What about right employee, right information, wrong use?

- **Managing minimum necessary for "non-routine" disclosures: How to manage individual review?**
  - Large/complex organization vs. small
  - How to limit the information disclosed
  - Tracking and providing notice
  - Privacy oversight: de-centralized by task vs. central infrastructure

Minimum Necessary Requirements

- **In General:**
  - **How to ensure all requirements are met?**
    - > Are you required to track and monitor ***all*** internal use in order to identify inappropriate use?
    - > You are required to track external disclosures
  - **How to integrate the Security requirement for auditing access**
    - > How deep/extensive
    - > What to do with the audit data? Are you required to review and analyze?
- **Sources:**
  - *§164.502 Uses and disclosures of protected health information: general rules*
  - *§164.514 Other requirements relating to uses and disclosures of PHI*
  - *§ 164.504 Uses and disclosures: organizational requirements*
  - *HHS Guidance issued July 6, 2001*

Contents

- Common Themes from Privacy Assessments
- Complex Privacy Issues
- Issue Drill Down
- Potential Changes in the Privacy Rule

Potential Developments in the Privacy Rule

- **Privacy revisions are rumored to delay Privacy effective date, but--**
  - There will be no implementation delay in the HIPAA privacy rule. HHS says that April 14, 2003 is “cast in stone”.
- **There will be formal revisions of the Privacy rules, not another “Advisory”—**
  - In the form of a Notice of Proposed Rulemaking (NPRM)
  - Currently being reviewed by Office of Management and Budget
  - Release date sometime in the next several months

Potential Developments in the Privacy Rule (cont'd)

- The NPRM will formalize much of the "Advisory" published last year as well as provide additional clarifications and some relaxation. Expected content includes:
  - Allowing phoned-in prescriptions without obtaining prior written consent
  - Scheduling first time referral appointments without prior written consent
  - Allowing routine oral communications with family members and treatment discussions
  - Clarifying the scope of the minimum necessary requirements to allow certain common practices such as
    - Use of sign-up sheets
    - X-ray light boards
    - Maintenance of patient medical charts at bedside
  - Assure that parents have appropriate access to information about the health and well-being of their children.
  - Permit marketing activities without a prior authorization