HIPAA Standards Update

Centers for Medicare and Medicaid Services
Office of eHealth Standards and Services
March 2007

Claims Attachment

- Final rule in process
- HL7 process – technical comments
- Policy issues
  - Unsolicited attachments
  - Attachments in COB process

ICD-10

- Policy discussions continue
- Issues
  - Compliance date
  - Cost to industry
- 5010 status

Remote Access Security Guidance

- Supports policies and strategies for compliance with the HIPAA Security Rule
- Highlights three activities:
  1. Conducting Security Risk Assessments
  2. Developing and Implementing Policies and Procedures
  3. Implementing Mitigation Strategies
- Released December 28, 2006 at:
  - http://www.cms.hhs.gov/securitystandard/

Why a new guidance?

- Since the original rule there has been:
  - Changes in Technology
    - Increases in mobile devices Increased workforce mobility
    - Increased use of portable media
  - Recent Security Incidents
    - Reports of thefts of laptops and media containing EPHI
    - Reports of access to EPHI by unauthorized users
- The original rule was intentionally broad

What's Affected?

Devices, Media and Connectivity Tools:

- Laptops
- Home PCs
- PDAs
- Smart Phones
- Library, Hotel, and other public PCs
- Wireless Access Points
- USB Flash Drives
- CDs and DVDs
- Floppy Disks
- Backup Media
- Email
- Smart Cards
- Remote Access Devices
- Etc.

Guiding Principles

- Be deliberate about EPHI release
  - EPHI release should have a valid operational justification
- EPHI Release Requires:
  1. Risk Analysis
  2. Policy & Procedure Development
  3. Risk Mitigation Strategies

Risk Analysis

- Security compliance requires analysis of risks and mitigation factors
- Factors to consider in risk assessments, per § 164.306(b)(2):
  i. *The size, complexity, and capabilities of the covered entity.*
  ii. *The covered entity's technical infrastructure, hardware, and software security capabilities.*
  iii. *The costs of security measures.*
  iv. *The probability and criticality of potential risks to [EPHI].*

Policy Development

- Requires training and compliance
- Ongoing workforce awareness programs
- Guidance discusses three key areas:
  - Data Access
  - Data Storage
  - Data Transmission

Example Data Access Strategies

Risks

- Lost passwords
- Unauthorized access
- Unattended workstations and home computers
- Failure to log off public machines
- Viruses

Potential Mitigation Strategies

- Two-factor authentication
- Secure user names
- Clearance and training procedures for data use
- Limiting access to EPHI to users with specific requirements and authorization
- Session termination and timeouts for remote applications
- Personal firewall and antivirus software

Next Steps

- Notice of Proposed Rule Making to incorporate guidance into the Security Rule

NPI Implementation

- Status
  - May 23, 2007 compliance date (for all but small plans)
  - Over 1.9 million providers enumerated (of an estimated 2.3 million universe)
  - Data dissemination notice under review by OMB

NCVHS Hearings

- Testimony from broad spectrum of stakeholders
- Consensus:
  - Much progress toward compliance BUT
  - Many covered entities will not meet May 23 date
  - Situation is similar to 2003, when HHS declared contingency for transactions and code set standards

Specific Issues

- Complexity of building and testing crosswalks between NPIs and legacy ID's
- Some providers have not gotten their NPIs, most are not submitting them on transactions
- Outreach and education efforts have not reached all affected entities

Specific Issues (cont'd)

- Mechanisms needed to promote easy access for providers to NPIs of other providers
  - Labs and DME suppliers need NPI of referring provider
  - Hospitals need NPI of operating physician
  - Pharmacies need NPI of prescriber

NCVHS Recommendations

- Adopt contingency guidance similar to 2003
  - Covered entities can adopt contingency plans to work with noncompliant trading partners to work toward compliance without jeopardizing cash flows
  - In event of complaint, CMS would assess “good faith efforts”

NCVHS Recommendations (cont'd)

- Contingency period would end 6 months after later of:
  - May 23, 2007
  - First date where NPPES data available
- Time limited contingency encourages continued movement toward compliance

NCVHS Recommendations (cont'd)

- Did not specify what a contingency plan would look like (e.g., did not require ability to process both NPI and legacy ID's)
- Did reflect expectation that providers should obtain and use NPI asap and that plans should be ready to accept them asap

NCVHS Recommendations (cont'd)

- Publish Data Dissemination Notice asap AND make data available as soon thereafter as possible
- Continue outreach and education, in particular to provider community

Next Steps

- Watch CMS website, listservs, etc. for further information
- Plans should consider possibility of contingency in event of guidance
  - What would contingency be, how would it be communicated?