HIPAA Security Overview

National Institute for Standards and Technology
January 16, 2008

Tony Trenkle, Director – Office of E-Health Standards and Services (OESS)

Centers for Medicare & Medicaid Services (CMS)

Agenda

- Role of CMS/OESS
- Security Rule Overview
- Remote Use & Access Guidance
- HIPAA Security Enforcement
- Compliance Reviews
- Q&A

Role of CMS/OESS

- CMS has delegated authority to enforce the non-privacy provisions of the HIPAA regulations:
  - Transactions and Code Sets
  - Identifiers
  - Security
- OESS is responsible for HIPAA enforcement as well as:
  - Regulatory/Policy Interpretation
  - Outreach and Education
    - Guidance and FAQs
  - New Regulations (including other ehealth related issues e.g. eRx)

Outreach and Education Efforts

- Federal and Non-Federal Collaboration
  - NIST, OCR, OIG, WEDI, BCBSA, MGMA…
- Promote Educational & Guidance materials
  - Security Papers
    1. Safeguards: Administrative, Physical and Technical
    2. Organizational Policies
    3. Basics of Risk Analysis and Risk Management
    4. Implementation for the Small Provider
  - Remote Use and Access Guidance
  - Frequently Asked Questions

Security Rule Overview

- Applies to Electronic Protected Health Information (EPHI) that a covered entity creates, receives, maintains, or transmits
- Scalability/Flexibility
  - Based on organization size, complexity, technical capabilities and infrastructure, cost of security measures and potential security risks
- Technologically Neutral
  - Describes “what” needs to be done vs. “how” it is to be done
- Standards are required but the implementation specifications may be either required or addressable

Rationale for Remote Use & Access Guidance

- **Increased risk to protected health information**
  - Associated with increased remote access to EPHI
  - Increase in workforce mobility
  - Increase in use of portable media storage devices
- **Recent security related incidents**
  - Reported loss or theft of devices containing EPHI
  - Reported access to health information by unauthorized users

Highlights of Remote Access Guidance

- Published December 28, 2006
- Reiterates requirements of the HIPAA Security Rule
- Identifies strategies consistent with organizational capabilities
- Pertains to Access, Storage and Transmission of EPHI
- Three categories of action highlighted:
  1. Conducting Security Risk Assessment
  2. Developing and Implementing Policies and Procedures
  3. Implementing Mitigation Strategies

HIPAA Security Enforcement – Current Process

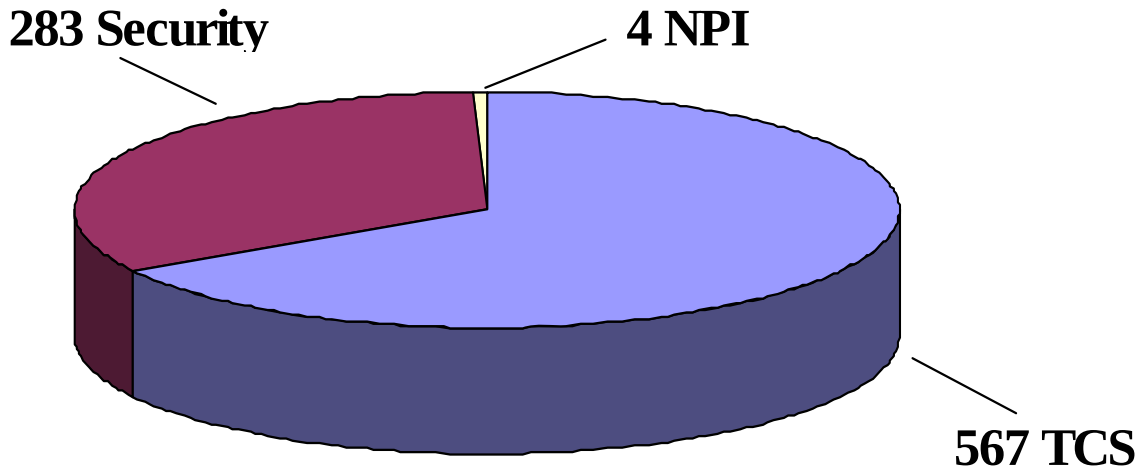
- Review complaint to determine validity and scope
- Notify “Filed Against Entity” (FAE) of complaint
- Request specific documents from the FAE
- Assess documents to determine if they:
  1. demonstrate compliance
  2. demonstrate the need for a Corrective Action Plan (CAP)
- Monitor CAPs to completion
- Close complaint upon demonstration of compliance
- Issue closure correspondence to all parties

Complaints with combination of Security and Privacy violations

- OESS and the Office for Civil Rights (OCR) collaborate on cases that overlap the Security and Privacy Rules
- Approximately 70% of the OESS Security cases are referrals from OCR
- Majority of Security complaints – allegation of inappropriate access and risk of inappropriate disclosure

HIPAA Enforcement Statistics

Open and closed cases as of December 31, 2007



Complaint Type	Open	Closed	Totals
Transactions and Code Sets (TCS)	52	515	567
Security	92	191	283
National Provider Identifier (NPI)	0	4	4
Total	**144**	**710**	**854**

Note: 49 of 283 of the closed Security cases have been closed via corrective actions.

HIPAA Security Complaint Categories

- Unauthorized access to EPHI
  - Employees or relatives accessing EPHI
- Loss or theft of devices containing EPHI
  - Small volume of complaints; large volume of records
- Insufficient access controls for systems containing EPHI
  - Shared passwords
  - Generic user Ids
  - encryption

Upcoming HIPAA Security Enforcement Initiatives

- CMS has the authority to conduct compliance reviews
  - Enforcement Rule: 45 CFR §§160.300-160.316
- CMS contracted with Price Waterhouse Coopers (PwC) to assist with onsite reviews
- Covered entities must provide access to facilities, records and other information
- Initial target:
  - entities against whom a complaint has been filed and
  - Risk to high volume of records is deemed moderate to high

Discussion and Questions