HIPAA Security Rule Implementation and Compliance Status Report

Tenth National HIPAA Summit
April 7, 2005

Brad Peska, CISSP
Office of HIPAA Standards (OHS)

Agenda

- OHS Overview
- Non-Privacy Enforcement Procedures
- HIPAA Security Enforcement Approach
- HIPAA Security and Privacy Enforcement Coordination
- HIPAA Security Outreach Activities
- CMS/OHS HIPAA Resources
- Questions

Office of HIPAA Standards - Enforcement Role

- Centers for Medicare and Medicaid Services (CMS), Office of HIPAA Standards (OHS)

- Develops, implements and administers the enforcement of the HIPAA including;
  - Transactions and Code Sets
  - Identifiers
  - Security

HIPAA Non-Privacy Enforcement Procedures

- CMS Federal Register Notice; March 25, 2005 (70 FR 15329 – 31)
  - "Procedures for Non-Privacy Administrative Simplification Complaints Under the Health Insurance Portability and Accountability Act of 1996"

HIPAA Non-Privacy Enforcement Procedures

- HIPAA Administrative Simplification (A.S.) Non-Privacy Regulations
  - Transaction and Code Set Rule (TCS), 65 FR 50313 (August 17, 2000)
  - National Employer Identifier Number (EIN) Rule, 67 FR 38009 (May 31, 2002)
  - Security Rule, 68 FR 8334 (February 20, 2003)
  - National Provider Identifier Rule, 69 FR 3434 (January 23, 2004)
  - National Plan Identifier Rule (currently under development)

HIPAA Non-Privacy Enforcement Procedures

- Who can file?
- Who can be filed against?
- How do you file?
    1. Internet using the Administrative Simplification Enforcement Tool (ASET): https://htct.hhs.gov/
    2. Mail: Centers for Medicare & Medicaid Services, HIPAA TCS Enforcement Activities, P.O. Box 8030, Baltimore, MD 21244–8030
- When can you file?

HIPAA Non-Privacy Enforcement Procedures

- Complaints must meet all of the following requirements:
  - Be filed in writing, either on paper or electronically. CMS will not accept faxed complaints.
  - Describe the acts or omissions believed to be in violation of the applicable administrative simplification provisions.
  - Provide contact information, including name, address, and telephone number, for the complainant and the covered entity that are the subject of the complaint.
  - Be filed within 180 days of when the complainant knew or should have known that the act or omission that is the subject of the complaint occurred, unless this time limit is waived by CMS for good cause shown.

HIPAA Non-Privacy Enforcement Procedures

- After receiving a complaint, CMS will:
  - Acknowledge receipt within 14 days
  - Perform an initial review
  - Accept or Deny Complaints

HIPAA Non-Privacy Enforcement Procedures

- A complaint may be withdrawn at any time, upon notice to CMS
- Even if a complaint is withdrawn, CMS may continue its investigation
- In general, a withdrawn complaint may be re-filed; subject to 180 day requirement

HIPAA Non-Privacy Enforcement Procedures

- If a complaint is accepted, CMS will:
  - Begin an investigation
  - Request additional information from complainant

HIPAA Non-Privacy Enforcement Procedures

- If CMS ascertains that a compliance failure by a covered entity may have occurred, CMS will;
  - Advise the covered entity that a complaint has been filed
  - Inform the covered entity of the alleged compliance failure

HIPAA Non-Privacy Enforcement Procedures

- Primary approach is to obtain voluntary compliance
- CMS will ask the covered entity to respond to the alleged compliance failure by submitting in writing:
  - (1) A statement demonstrating compliance; or
  - (2) a statement setting forth with particularity the basis for its disagreement with the allegations; or
  - (3) a corrective action plan

HIPAA Non-Privacy Enforcement Procedures

- Covered entities will generally have 30 days to respond to CMS' request for information
- A covered entity that disagrees with the allegations made should set forth and document, where possible:
  - (1) Compliance;
  - (2) in what respect it believes the allegations to be factually incorrect or incomplete; and/or
  - (3) why it disagrees that its alleged actions or failures to act constitute a failure to comply

HIPAA Non-Privacy Enforcement Procedures

- Upon receipt of this response from the covered entity, CMS may:
  - Communicate with the covered entity and request interviews or additional documents or materials
  - Seek additional information from the complainant
- A covered entity may, at any time:
  - Amend or supplement its response
  - Propose voluntary compliance through a corrective action plan

HIPAA Non-Privacy Enforcement Procedures

- If the covered entity comes into voluntary compliance, CMS will notify the complainant by mail or electronically.
- CMS may issue an investigational subpoena in accordance with 45 CFR 160.504
- After finding that a violation exists, the Secretary will pursue other options, such as, but not limited to, civil money penalties
- The parties to the complaint will be notified, as appropriate, when the complaint is closed

HIPAA Security Enforcement Approach

- Compliance Date: No later than April 20, 2005; (small health plans, no later than April 20, 2006)
  - No plans for an extension of this date
- CMS will begin accepting Security Rule complaints on April 21, 2005
- Primarily a complaint driven process
- CMS will focus on obtaining voluntary compliance

HIPAA Security and Privacy Enforcement Coordination

- Actively working with the Office for Civil Rights (OCR) on HIPAA enforcement issues
  - Overlap between the HIPAA Security and Privacy Rules
  - Collaboration during HIPAA Security and Privacy enforcement

HIPAA Security Outreach Activities

- CMS/OHS Website
  - HIPAA Security FAQs
  - “HIPAA Security Series” Educational Papers
  - HIPAA Outreach Distribution List
  - askHIPAA@cms.hhs.gov
  - Other Educational Materials

- National HIPAA Security Roundtable
  - April 13, 2005 at 2:00PM ET
  - (877) 203-0044 ID#: 4587639

CMS/OHS HIPAA Resources

- http://www.cms.hhs.gov/hipaa/hipaa2/ - CMS HIPAA Administrative Simplification Website for Electronic Transactions and Code Sets, Security, and Unique Identifiers

- https://htct.hhs.gov - HIPAA Administrative Simplification Enforcement Tool (ASET) electronic complaint submission

Questions

Brad Peska, CISSP
Security Specialist
Office of HIPAA Standards
bpeska@cms.hhs.gov
(410) 786-4160