HIPAA
Privacy Rule Compliance Issues

Presentation for AAPM

Myra N. Moran J.D.

HHS/OCR August 2, 2006

DISCLAIMER

My goal in speaking with you today is to explain Privacy Rule compliance issues. I can make factual statements, including pointing to formal interpretations of the Office for Civil Rights (OCR), but I am unable to provide official interpretations of the Rule. To the extent that I provide interpretations in this presentation, those interpretations are solely my individual opinion and do not represent official interpretations of the Department of Health and Human Services.

Office for Civil Rights

- Enforces Civil Rights laws and the Privacy Rule

Ten Regions

- Ten regional offices-each covers multiple states.
- Region IV-Georgia, Florida, Tennessee, Mississippi, Alabama, North Carolina, South Carolina, and Kentucky.
- Regional Manager and EOS staff
- HQ Compliance Advisor

Compliance and Enforcement

- Technical assistance for voluntary compliance
- Any person or organization can file complaints with OCR (generally within 180 days)
- OCR may investigate complaints and may conduct compliance reviews
- OCR shall attempt to resolve noncompliance by informal means

HIPAA Privacy Rule Complaints Received

Year (calendar)	Receipts	Closed (April 14, 2003 to June 30, 2006)
2003	3,745	
2004	6,507	
2005	6,886	
2006 (as of June 30, 2006)	3,709	
Total	**20,847**	**75%**

Most Complaints Are Filed Against These CEs

1. Private health care practices
2. General hospitals
3. Outpatient facilities
4. Group health plans and health insurance issuers
5. Pharmacies

Top Complaint Allegations

1. Impermissible use or disclosure of an individual's identifiable health information
2. The lack of adequate safeguards to protect identifiable health information
3. Refusal or failure to provide the individual with access to or a copy of his/her records
4. The disclosure of more information than is minimally necessary to satisfy a particular request for information
5. Failure to have the individual's valid authorization for a disclosure that requires one

Enforcement Rule Key Dates

- **Proposed rule published April 18, 2005**
  (70 FR 20224)
- **Final rule published February 16, 2006**
  (71 FR 8390)
- **Effective March 16, 2006**
- **Applicable to all Administrative Simplification Rules**
  - **Privacy Rule (OCR)**
  - **Security Rule (OESS/CMS)**

What Does the Enforcement Rule Do?

- **Establishes requirements for investigation and informal resolution of compliance issues**
- **Establishes procedures for imposition of a civil money penalty (CMP) when a compliance issue is not resolved informally**
- **Defines basis for liability for a CMP; how CMPs are calculated; defenses that** can **be raised to the imposition of a CMP**

What Does the Enforcement Rule Do?
(cont'd)

- Strengthens OCR's authority to enforce Privacy Rule
- Requires OCR to attempt to reach a resolution of the matter satisfactory to the Secretary by informal means, including demonstrated voluntary compliance or completed corrective action plan (45 CFR 160.312)
- CMPs can be imposed by OCR in a Notice of Proposed Determination:
  - $100 per violation; capped at $25,000 for each calendar year for each identical requirement or prohibition that is violated;
  - Covered entity has a right to notice and a hearing before a CMP becomes final

Why Informal Resolution of Complaints and Compliance Reviews?

- Most effective way to obtain industry compliance with the Privacy Rule
- Most prompt for all: complainants, covered entities, and OCR
- Most efficient use of enforcement resources
- Can help mitigate civil money penalties (CMPs) on irresolvable issues
- Resolution must be satisfactory to the Secretary

OCR Referrals to Department of Justice

- Section 1177 of HIPAA (42 USC 1320d-6) defines HIPAA criminal violations: A person who knowingly and in violation of the Privacy Rule discloses or obtains individually identifiable health information
- OCR refers complaints alleging actions that meet these requirements to DOJ for review - 332 as of June 30, 2006
- DOJ accepts or declines for prosecution
- OCR receives DOJ declined cases for administrative enforcement

OCR Referrals to CMS/OESS

- OCR refers complaints alleging actions that would violate the Security Rule to the Office of E-health Standards and Services (OESS) of CMS
- There is a coordinated investigative and enforcement process for complaints that allege facts that may be potential violations of the Privacy Rule and Security Rule
- For example, notification letter to the CE will mention both rules and indicate that OCR is the lead agency for communications (such as data requests) with CE
- Each agency retains its own authority to investigate compliance with its rule and make its own determination (e.g., no violation, informal resolution, or CMP)

§ 160.402(c) – Liability for Acts of Workforce

- A workforce member is an agent of the covered entity, and the CE is liable for the violations by its agents within the scope of their agency.
- Employees, volunteers, and trainees will always be workforce members.
- Independent contractors may be workforce members, but more likely are business associates; the issue is whether they are under the direct control of the CE.

Business Associates

- Agents, contractors, others hired to do work of or for covered entity that requires use or disclosure of protected health information
- Require satisfactory assurance – usually a contract – that a business associate will safeguard protected health information, limit use and disclosure

§ 160.402(c) – Liability for Acts of Business Associates

- Whether a business associate is an agent of the CE must be determined.
- A CE is liable for a violation by a business associate agent, unless it is in compliance with the business associate provisions of the Privacy Rule, i.e.–
  - It has a business associate contract or other arrangement in place that complies with § 164.504(e); and
  - It did not know of the violation; or
  - If it knew of the violation, has taken steps as required by § 164.504(e)(1)(ii).

§ 160.410 – Affirmative Defenses

- An affirmative defense is a defense which, if shown, bars imposition of the CMP.
- Three statutory affirmative defenses:
  - The act is a criminal offense under HIPAA;
  - The CE lacked knowledge of the violation; or
  - The violation was due to reasonable cause and not willful neglect and is timely corrected.
- The second and third affirmative defenses are waived if not raised in the RFH; the first affirmative defense may be raised at any time.

Tips for CE Privacy Officers During an OCR Investigation

- Not all cases result in an investigation
  - First, desk review of complaint; contact with complainant; may be closed at this point if alleged facts would not be a violation
  - Notification letter to CE signals formal investigation
- When notification letter is received, contact investigator named in letter. Establish effective communication with investigator. Contact investigator for assistance with questions, such as, “How does this work…?”
- Respond within stated time frames. If CE cannot make the due date, let investigator know. Request a reasonable extension of time – enough so CE can accomplish the requested task. Avoid multiple requests for time extensions. Return telephone calls from the OCR investigator promptly.

Tips for CE Privacy Officers During an OCR Investigation (cont'd)

- If CE is aware of a Privacy Rule incident even before receiving notification letter, start gathering relevant materials and facts. Formulate corrective action plan (CAP) and execute it. An executed CAP will then be ready to deliver to the investigator when notification letter is received.
- Be specific in your responses to requests for data and information. For example, if training was provided, provide all the facts – when, who was trained (sign-in sheet), topics covered; if a policy has been revised, send a copy of the old policy and the new policy. Do not send entire privacy policies and procedures manual unless specifically requested.

Tips for CE Privacy Officers During an OCR Investigation (cont'd)

- **Understand that investigations take place over an extended period of time. OCR investigator will work hard to be timely, but some investigations take longer than others.**
- **Be cooperative with the OCR investigator. Facts need to be confirmed by OCR. If OCR requests to interview an employee or requests contact information for former employees, provide this information in a timely manner. If you cannot, explain why.**
- **Ask for technical assistance if you do not understand what is expected by a particular requirement of the Privacy Rule.**

Tips for CE Privacy Officers During an OCR Investigation (cont'd)

- **Be forthcoming and acknowledge errors if they occurred. Remember, the goal is informal resolution through voluntary compliance and completed corrective action.**
- **Respond. Ignoring the investigation will exacerbate the matter.**

Our Mutual Goal

- **Ensuring the privacy of each individual's health information in accordance with the standards and requirements of the HIPAA Privacy Rule**

Additional Information

www.hhs.gov/ocr/hipaa/