HIPAA Enforcement Update

Doris Genco
Office for Civil Rights
U.S. Department of Health and Human Services

October 26, 2012

What is OCR?

- OCR’s first national director was Leon Panetta, who is currently serving as Secretary of Defense.
- Over time, OCR received jurisdiction over a number of anti-discrimination statutes, including Section 504 of the Rehabilitation Act of 1973, Title II of the Americans with Disabilities Act, and the Age Discrimination Act of 1975.
- In 2000, OCR was designated as the agency within HHS which would administer and enforce the Privacy Rule. In 2009, OCR succeeded CMS as the agency that enforces the Security Rule.
- OCR also enforces the privilege and confidentiality protections of the Patient Safety Act.
Recent Enforcement Actions

OCR

Methods of Enforcement

- When OCR determines from its investigation of the allegations raised in a HIPAA complaint or through a compliance review that a covered entity may well have violated the Privacy Rule and/or the Security Rule, OCR has various means of enforcement at its command.
- If feasible, OCR usually seeks voluntary compliance. Voluntary compliance often involves the covered entity changing its policies and procedures, retraining personnel, and sanctioning the members of its workforce who violated the Privacy or Security Rules.
### Methods of Enforcement

- If OCR determines that the conduct involved warrants some sort of penalty even if voluntary compliance is forthcoming, OCR may seek to have the covered entity enter into a Resolution Agreement and Corrective Action Plan as well as pay a “resolution amount.” This method is often used when the problems identified by OCR are systemic.
- If OCR either determines that the conduct involved is so serious or if the covered entity is adamant in its refusal to cooperate in the investigation or resolution of the problem, OCR will assess a Civil Money Penalty (CMP).

---

### What is a Resolution Agreement?

- A settlement agreement between HHS and covered entity
- It incorporates a Corrective Action Plan which:
  - Generally lasts for three years;
  - Requires the covered entity to prepare new policies and procedures, subject to OCR approval;
  - Generally requires improved training; and
  - Requires monitoring of implementation and compliance
- Includes payment of a resolution amount
What is a Resolution Agreement?

- A Resolution Agreement and Corrective Action Plan do not constitute:
  - A formal finding of facts
  - A formal finding of a violation
  - An admission by the covered entity
- A “Resolution Amount” is not a civil monetary penalty, fine, or other formal penalty.
- Because a Resolution Agreement is an informal resolution into which the covered entity enters in lieu of administrative litigation:
  - The covered entity has no right to formal process or an administrative hearing.

How does RA/CAP Differ from Other Types of Informal Resolution?

- Usually investigations in which there are indications of noncompliance are concluded when:
  - The covered entity completes certain voluntary compliance actions to the satisfaction of OCR; and
  - OCR notifies the complainant and the covered entity in writing of the resolution result.
- The Resolution Agreement/Corrective Action Plan approach is generally designed for cases with systemic issues where entity-wide change in policy and procedures and in the internal emphasis placed on the issue is needed to ensure compliance.
Recent Enforcement Actions

HITECH has allowed the HHS Secretary to impose significantly increased penalty amounts for violations of the HIPAA rules and encourages prompt corrective action.

Implementation of HITECH Act enforcement strengthened the HIPAA protections and rights related to an individual’s health information.

This strengthened penalty scheme will encourage covered entities and business associates to comply with the HIPAA Privacy and Security and HITECH requirements.

OCR

Facts of Providence Health and Services Case

• Providence is a fairly extensive health care system based in Seattle, Washington
• Series of five incidents occurring between September 2005 and March 2006
• Incidents giving rise to the agreement involved two entities within the system
  • Providence Home and Community Services and
  • Providence Hospice and Home Care

OCR
Facts of Providence Health and Services Case

- On or about December 30, 2005, electronic protected health information ("ePHI") on four backup tapes and two optical disks were left unattended overnight in the personal vehicle of an employee and were stolen.

- The employee took the disks and tapes from Providence Home and Community Services ("HCS"), a division of PHS-Oregon, pursuant to a practice followed at the time by HCS Information Staff with the knowledge of some HCS managers.

- The ePHI on the tapes and disks was not encrypted.

Facts of Providence Health and Services Case

- Further, on the following dates, laptops containing ePHI were left unattended and were stolen from workforce members:
  - The ePHI on the stolen laptops was not encrypted.
Providence Investigation

- The investigation was triggered by 31 complaints submitted to OCR and the Centers for Medicare and Medicaid Services (CMS).
- The complaints were merged into a joint compliance review by CMS and OCR.
- It was determined that the practices of the Providence entities created systemic vulnerabilities that led to massive losses of ePHI.
- Providence was cooperative throughout the investigation.
- Providence executed a Resolution Agreement and Corrective Action Plan in July 2009.

OCR

“Indications” of Noncompliance in the Providence Resolution Agreement

- OCR cited the following “indications” of noncompliance in the Resolution Agreement:
  - ePHI was not encrypted or otherwise properly safeguarded by Providence.
  - Backup tapes, optical disks, and laptops, all containing unencrypted ePHI, were removed from the Providence premises by members of the Providence workforce and left unattended in vehicles.
  - Portable media and laptops were lost or stolen, compromising the ePHI of over 386,000 patients.
  - Providence management knew of such practices, but allowed them to continue.
Actions to Settle Providence Case

- Providence paid a $100,000 resolution amount.
- Providence’s Corrective Action Plan provided:
  1. Providence would revise its policies and procedures, subject to OCR approval, by:
     - Adopting new risk assessment and risk management tools
     - Improving physical and technical safeguards (e.g., encryption) for off-site transport and storage of electronic media containing PHI
  2. Providence would train its workforce members on electronic and other safeguards for PHI.
  3. Providence would conduct internal audits and site visits of facilities to determine compliance with the Corrective Action Plan.
  4. Providence would submit implementation report and annual reports to HHS for a period of three years.

Lessons Learned

- Effective compliance means more than just written policies and procedures.
- Corporate management of covered entities need to continuously monitor implementation of privacy and security policies and practices.
- HHS is willing to work with cooperative entities to implement effective changes to ensure that consumers are protected.
- Covered entities need to ensure that these efforts include:
  - Effective privacy and security staffing
  - Adequate employee training on privacy and security issues
  - Physical and technical implementation in an effective manner
Cignet Health Care

- Cignet Health Care is a treatment provider and health plan issuer
- Over a two-year period, 41 individuals complained to OCR that Cignet had ignored their requests for access to their health records
- Cignet failed to respond to OCR’s investigation or provide copies of the patients’ records

OCR

CMP of $4.3 Million Levied

- Civil Money Penalty of $1.3 million attributable to failure to provide individuals access to their health records
- Penalty of $3 million for failure to respond to OCR demands to produce records and failure to cooperate with OCR’s investigation

OCR
<table>
<thead>
<tr>
<th>Massachusetts General Hospital</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Large multi-specialty healthcare provider</td>
</tr>
<tr>
<td>• Employee, who had taken patient files home, left the folders on the subway train and they were never recovered</td>
</tr>
<tr>
<td>• Investigation initiated after media reports of incident and a complaint from an individual whose PHI was lost</td>
</tr>
<tr>
<td>• Settled with OCR through Resolution Agreement and corrective action plan</td>
</tr>
</tbody>
</table>

**Actions to Settle Case**

- $1 million resolution amount
- Corrective Action Plan
- MGH required to actively monitor its compliance with the Corrective Action Plan through use of an internal monitor
Management Services
Organization of Washington

• MSO provided practice management services to individual health care providers
• Affiliated company, Washington Practice Management, markets and sells Medicare Advantage plans to consumers for which it earns commissions
• Separate agreements with DOJ and OIG to settle allegations under the Federal False Claims Act

Indications of Noncompliance WA
MSO Resolution Agreement

• MSO disclosed ePHI to WPM, without a valid authorization, so that WPM could market Medicare Advantage plans to those individuals
• MSO had not developed or implemented appropriate and reasonable administrative, technical, and physical safeguards to protect ePHI
Actions to Settle Case

• $35,000 resolution amount to OCR
• Corrective Action Plan
  – Develop and implement policies & procedures to demonstrate compliance with the Privacy and Security Rules
  – Train workforce members
  – Conduct internal monitoring
  – Submit compliance reports to HHS for a period of two years

OCR

Rite Aid Corporation

• Large US pharmacy chain
• Series of media reports about personnel disposing of PHI, including labeled pill bottles and prescriptions, in unsecured garbage containers outside of several Rite Aid pharmacy stores
• Settled with OCR through Resolution Agreement and corrective action plan
• Simultaneously settled with FTC through a consent order

OCR
### Indications of Non-Compliance in Rite Aid Resolution Agreement

- Rite Aid policies and procedures for disposal did not reasonably and appropriately safeguard PHI
- Rite Aid did not maintain a sanctions policy for workforce members who failed to safeguard PHI in disposal process
- Rite Aid did not provide necessary and appropriate training for its workforce regarding disposal of PHI

*OCR*

### Actions to Settle Case

- $1 million resolution amount
- Corrective Action Plan
- Both HHS and FTC require RAC to actively monitor its compliance with the Resolution Agreement and Consent Order

*OCR*
Actions to Settle Case

1. Revising, distributing policies & procedures regarding PHI disposal
2. Sanctioning workers who do not follow them
3. Training workforce members
4. Conducting internal monitoring
5. Engaging a third-party assessor to render reports to HHS
6. New internal reporting procedures requiring workers to report all violations of these new privacy policies and procedures
7. Submitting compliance reports to HHS for a period of three years

OCR

A Culture of Compliance

• In light of OCR’s clearly articulated intention to aggressively enforce the HIPAA Privacy and Security Rules, covered entities and business associates should review their current HIPAA compliance programs.
• A robust compliance program includes employee training, vigilant implementation of policies and procedures, regular internal audits, and a prompt action plan to respond to incidents.

OCR
Want More Information?

The OCR website, http://www.hhs.gov/ocr/privacy/, offers a wide range of helpful information about health information privacy including educational information, FAQ’s, and rule text and guidance for the Privacy, Security, and Breach Notification Rules.