United States Department of Health & Human Services

Office of the Secretary

Office for Civil Rights (OCR)

Health Information Security Rule Trends in Enforcement

NIST/OCR HIPAA Security Assurance Conference

May 11, 2011

Sue McAndrew, JD

David S. Holtzman, JD

Office for Civil Rights

Health Information Privacy Division

Topics

- HIPAA Security Rule Enforcement Recap
- HITECH Breach Notification Recap
- Some Lessons Learned
- Resolution Agreements and CMPs
- Update on Recent Enforcement Actions

Your Health. Your Rights.

OCR's Vision:

Through investigations, voluntary dispute resolution, enforcement, technical assistance, policy development and information services, OCR will protect the civil rights of all individuals who are subject to discrimination in health and human services programs and protect the health information privacy rights of consumers.

Who We Are

- **Headquarters:**
  - Policy
  - Administration
  - Case management and oversight
  - External relations
- **10 HHS regional offices:**
  - Enforcement
  - Investigation
  - Compliance reviews
  - Public education and outreach
  - Technical assistance

Complaint Investigations

- Every complaint received is reviewed and the allegations are analyzed.
- Review for Privacy & Security Rule compliance in every breach report of >500
- OCR investigations have resulted in changes in privacy and information security practices and other corrective actions in over 13,300 cases since April 2003.
- Corrective action obtained by HHS from covered entities has resulted in systemic change

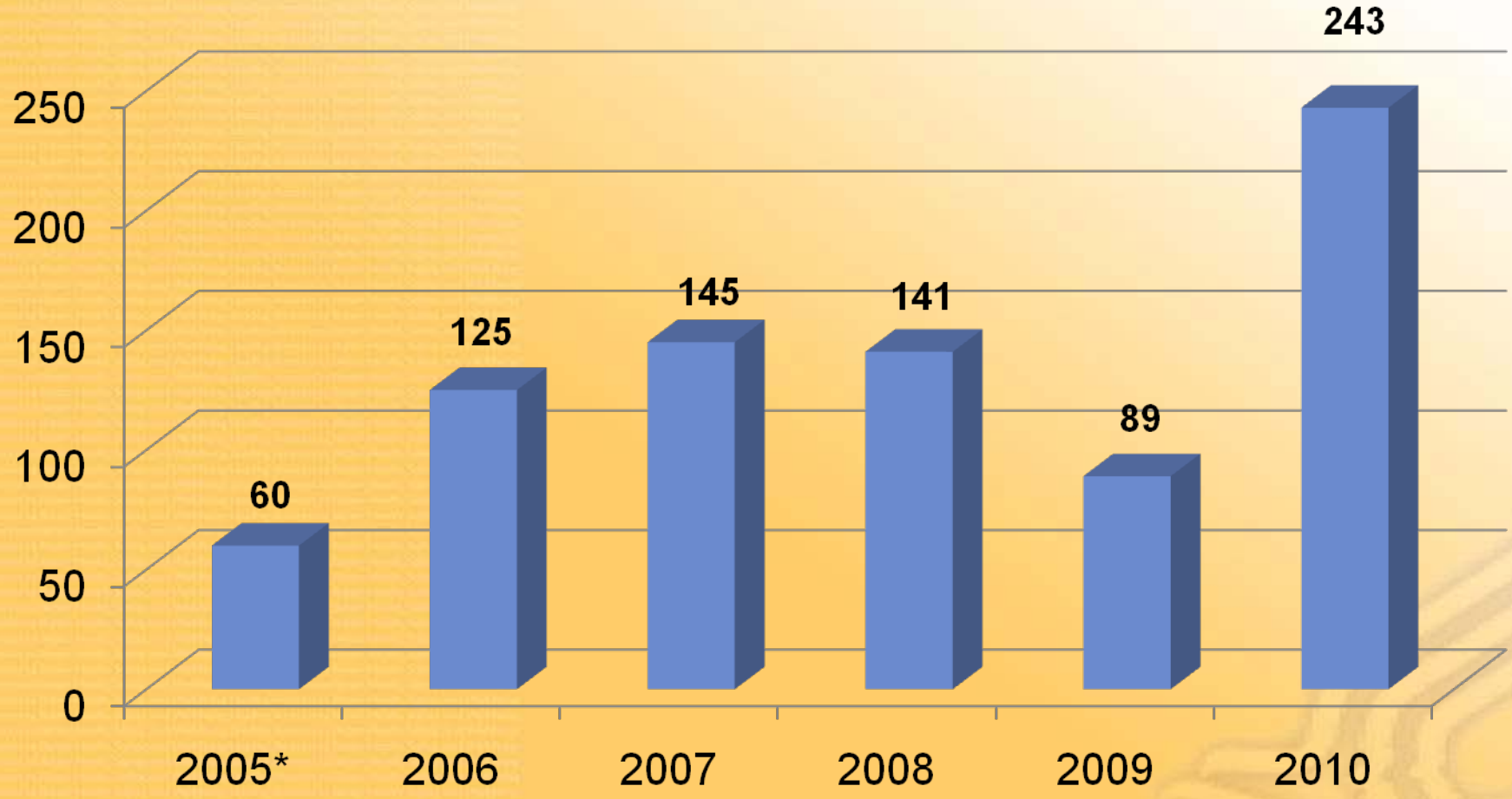
HIPAA Security Rule Enforcement

- Delegation of Authority – July 27, 2009
- Streamline, unify, simplify investigation and resolution of cases
  - Privacy Rule
  - Security Rule
  - Breach Notification
- Addresses overlap of security/privacy in HIT environment

HIPAA Security Rule Enforcement Activity

OCR

Security Complaints & Reviews Opened



*** Partial Year**

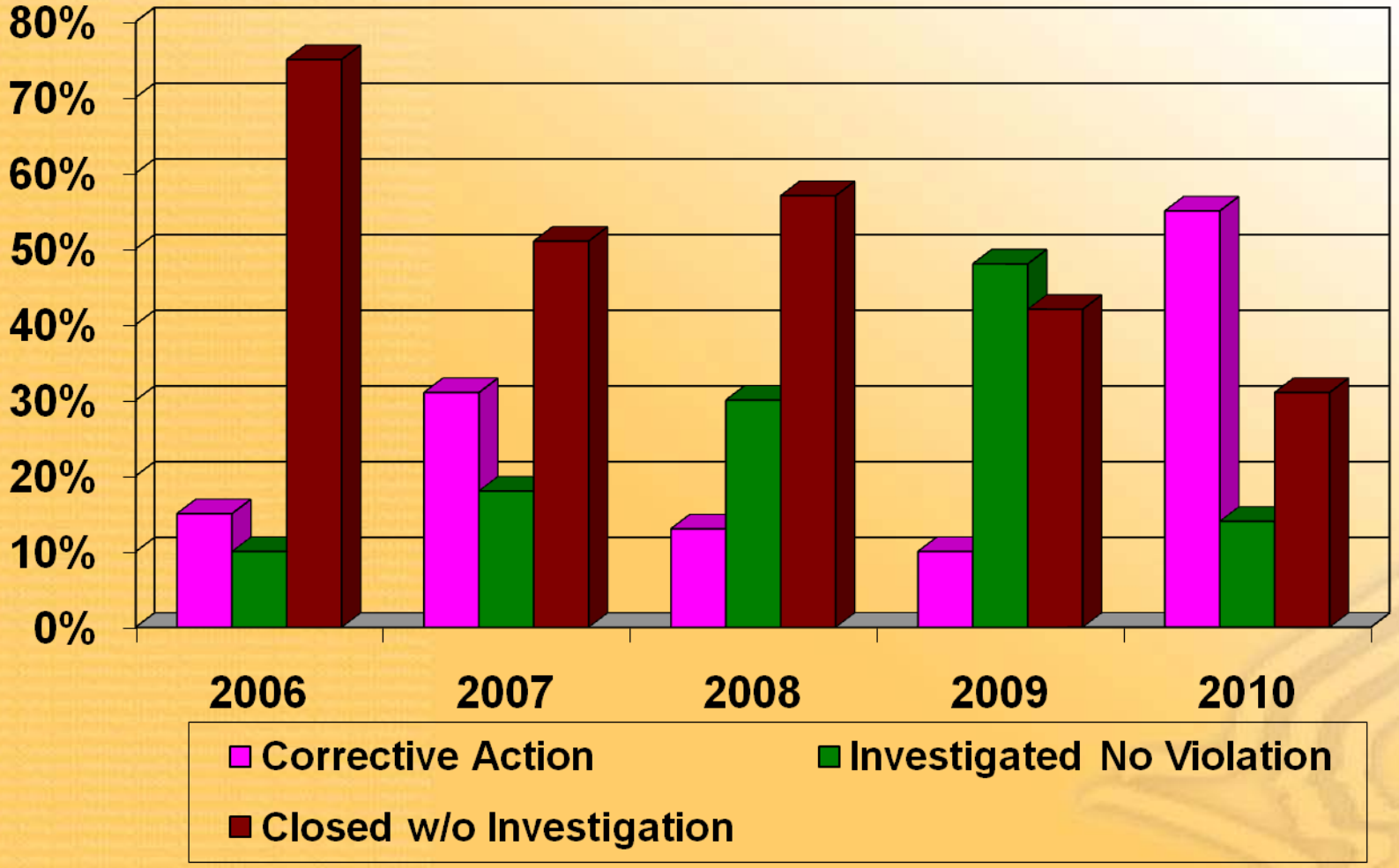
Security Rule delegated to OCR July 27, 2009

Security Complaints & Reviews Resolved

	2005	2006	2007	2008	2009	2010	TOTAL
Corrective Action	**0**	**9**	**41**	**21**	**9**	**70**	**150**
Investigated and No Violation Found	**0**	**6**	**24**	**50**	**41**	**18**	**139**
Closed Without Investigation	**7**	**44**	**68**	**93**	**36**	**40**	**287**
TOTAL:	***7***	***59***	***133***	***164***	***86***	***128***	***577***

Security Rule delegated to OCR July 27, 2009

Security Closures by Type



Most Frequent Security Rule Issues

Standard or Specification	Type of Safeguard	Count
Response and Reporting (R) 164.308(a)(6)(ii)	Administrative	179
Awareness & Training 164.308(a)(5)(i)	Administrative	144
Access Control 164.312(a)(1)	Technical	141
Information Access Management 164.308(a)(4)(i)	Administrative	126
Workstation Security 164.310(c)	Physical	84

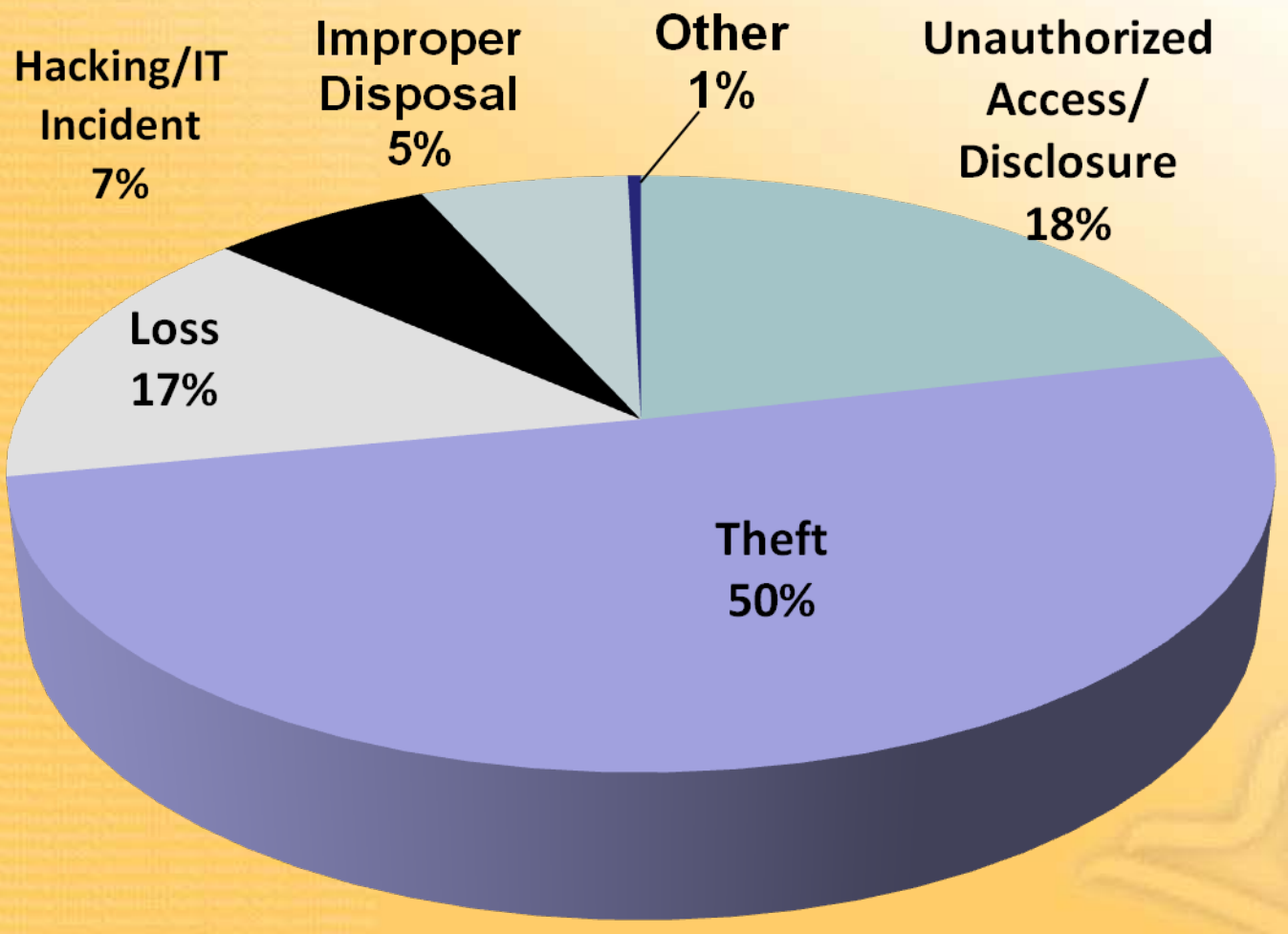
HITECH Breach Notification Rule Reports and Trends

Breach Notification Highlights

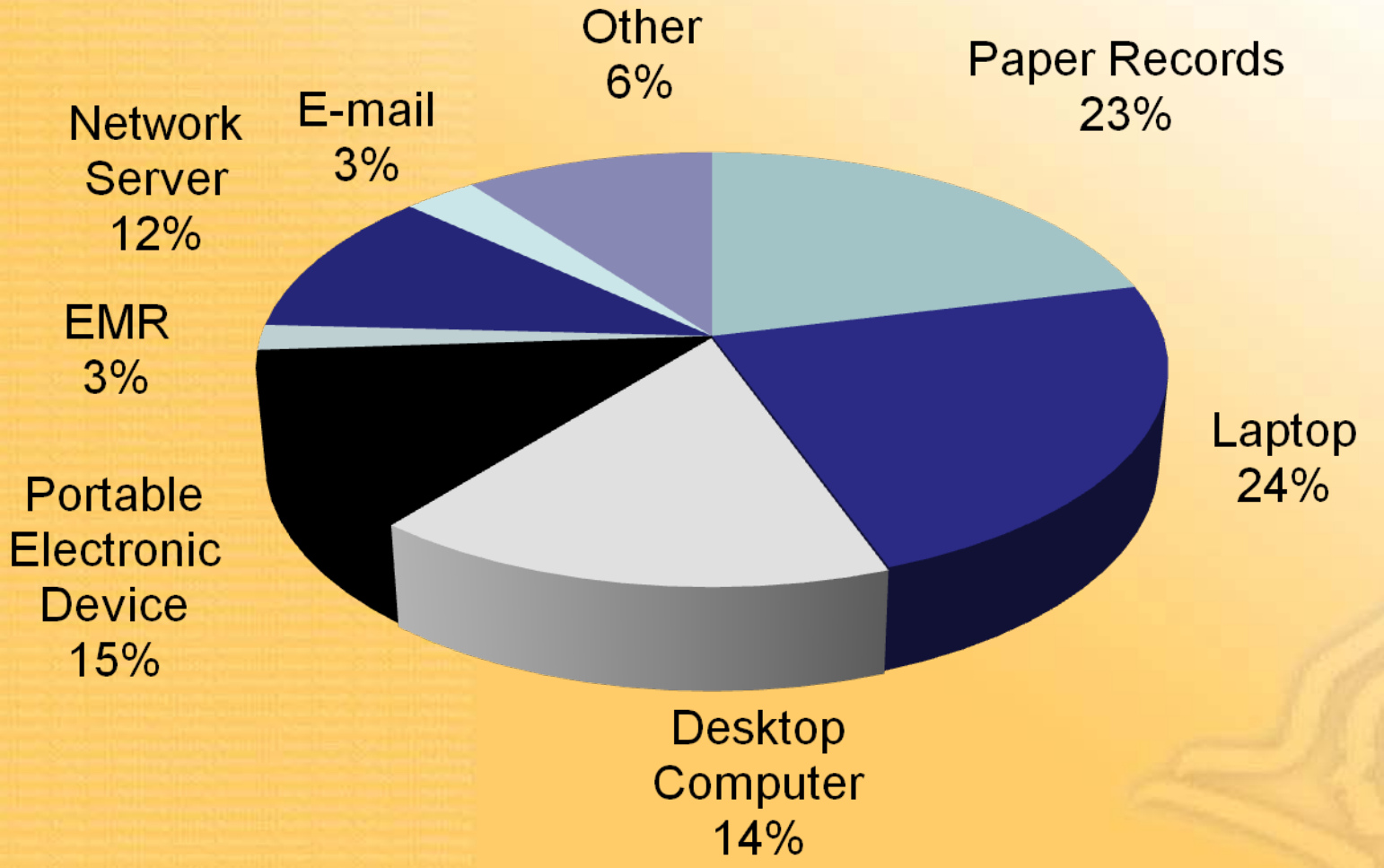
September 2009 through April 2011

- 265 reports involving a breach of over 500 individuals
  - Theft and Loss are 67% of large breaches
  - Large breaches involving portable storage devices and laptop or desktop computers account for 53% of large breaches
  - Paper records are 23% of large breaches
- 31,000+ reports of breaches of under 500 individuals

Breach Notification:
500+ Breaches by Type of Breach



Breach Notification:
500+ Breaches by Location of Breach



Lessons Learned

- Do not neglect physical safeguards for areas where paper records are stored or used
- Reduce risk through network or enterprise storage as alternative to local devices
- Encryption of data at rest on any desktop or portable device/media storing EPHI

Lessons Learned

- Clear and well documented administrative and physical safeguards for storage devices and removable media which handle EPHI

- Raise the security awareness of workforce members and managers to promote good data stewardship

Resolution Agreements and Civil Monetary Penalties

What is a Civil Monetary Penalty?

- Civil Monetary Penalty (CMP)
  - A formal finding of facts
  - A formal finding of a violation
- CMP amount for a violation can range based on the level of culpability
- Calculated per violation, per day
- CMP is a formal resolution:
  - Covered entity has right to due process as specified in Enforcement Rule
  - Covered entity has right to request an ALJ hearing

Amount of a Civil Monetary Penalty

Violation Category	**Each Violation**	**All Identical Violations per Calendar Year**
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 - $50,000	$1,500,000
Willful Neglect-corrected in 30 days	$10,000 - $50,000	$1,500,000
Willful Neglect-not corrected	$50,000	$1,500,000

What is a Resolution Agreement?

- Settlement agreement between HHS and covered entity
- 45 CFR 160.312 authorizes “other agreement” to resolve indications of violations
- Incorporates a Corrective Action Plan
  - Generally for three years
  - Policies and procedures, subject to HHS approval
  - Generally improved training
  - Monitoring of implementation and compliance
- Includes payment of a resolution amount

Resolution Through Informal Means

- *45 CFR 160.312*: If investigation or compliance review indicates noncompliance, HHS will attempt to reach resolution satisfactory to the Secretary by "informal means."
- "Informal means" includes:
  - Demonstrated compliance;
  - Completed corrective action plan; or
  - Other agreement.

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

- Usually investigations in which there are indications of noncompliance are concluded when:
  - The 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
- RA/CAP is for those cases where resolution satisfactory to OCR cannot be obtained through the entity's demonstrated compliance or corrective action

Recent Enforcement Actions

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 ignored their requests for access to their health records
- Cignet failed to respond to OCR's investigation or provide copies of the patient's records

CMP of $4.3 Million Levied

- Civil Monetary 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 or cooperate in the investigation

Massachusetts General Hospital

- Large multi-specialty healthcare provider
- Employee who had taken patient files home left the folders on the subway train and they were never recovered
- Investigation initiated after media reports of incident and a complaint from an individual whose PHI was lost
- Settled with OCR through Resolution Agreement and corrective action plan

Actions to Settle Case

- $1 million resolution amount
- Corrective Action Plan
- MGH required to actively monitor its compliance with the Corrective Action Plan through an internal monitor

Actions to Settle Case

1. Revising, distributing policies & procedures regarding safeguards applied to PHI & EPHI away from the premises of the CE
2. Sanctioning workforce members who do not follow them
3. Training workforce members
4. Conducting internal monitoring
5. Submitting compliance reports to HHS for a period of three years

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

A Culture of Compliance

- OCR aggressively enforcing the HIPAA Privacy and Security Rules
- Covered entities and business associates should have robust HIPAA Privacy and Security 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

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, rule text and guidance for the Privacy, Security, and Breach Notification Rules.