United States Department of Health & Human Services

HIPAA Security Rule Enforcement Update

NIST/OCR Safeguarding Health Information Conference
May 11, 2010

Marilou King, J.D.
Civil Rights Division, Office of General Counsel

David Holtzman, J.D.
Health Information Privacy Division, Office for Civil Rights

Enforcement Framework in Complaint Investigation

- The Enforcement Rule
  - 71 FR 8390 (Feb. 16, 2006)
  - Revised 74 FR 56123 (Oct. 30, 2009)
- Enforcement Rule modified to implement changes mandated by HITECH Act
- The Enforcement Rule applies to both the Privacy, Security, and Breach Notification Rules as well as other Administrative Simplification rules.

Modifications to the Penalty Scheme in Enforcement Rule

- Tiered Increase in Amount of CMPs:
  - Four categories of violations that reflect increasing levels of culpability;
  - Four corresponding tiers of penalty amounts;
  - Minimum penalty amount for each violation; and
  - A maximum penalty amount of $1.5 million for multiple violations of an identical provision in a calendar year.

Amount of a Civil Money Penalty

	For violations occurring prior to 2/18/2009	For violations occurring on or after 2/18/2009
Penalty Amount	**Up to $100 per violation**	**$100 to $50,000 or more per violation**
Calendar Year Cap for Multiple Violations of Identical Requirement	**$25,000**	**$1,500,000**

Amount of a Civil Money 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

Affirmative Defenses

Violations Occurring Before the HITECH Act (before February 18, 2009):

- Disclosure is punishable criminally under § 1177;
- CE did not know and reasonably would not have known that violation occurred; or
- Violation due to reasonable cause and not willful neglect, and corrected during 30-day time period.

Violations Occurring After the HITECH Act (on or after February 18, 2009):

- Disclosure is punishable criminally under § 1177 (until February 18, 2011); or
- Not due to willful neglect and corrected during 30-day time period.

Changes in Affirmative Defenses

- A covered entity that *"did not know"* of a violation can no longer claim an affirmative defense to the imposition of a penalty, UNLESS
- The covered entity has corrected the violation during 30-day time period - beginning on the date the covered entity knew, or, by exercising reasonable diligence, would have known of the violation.
- Violation due to reasonable cause and covered entity has corrected the violation during 30-day time period .

United States Department of Health & Human Services

How OCR Enforces the Security Rule

David Holtzman, J.D.
Health Information Privacy Division, Office for Civil Rights

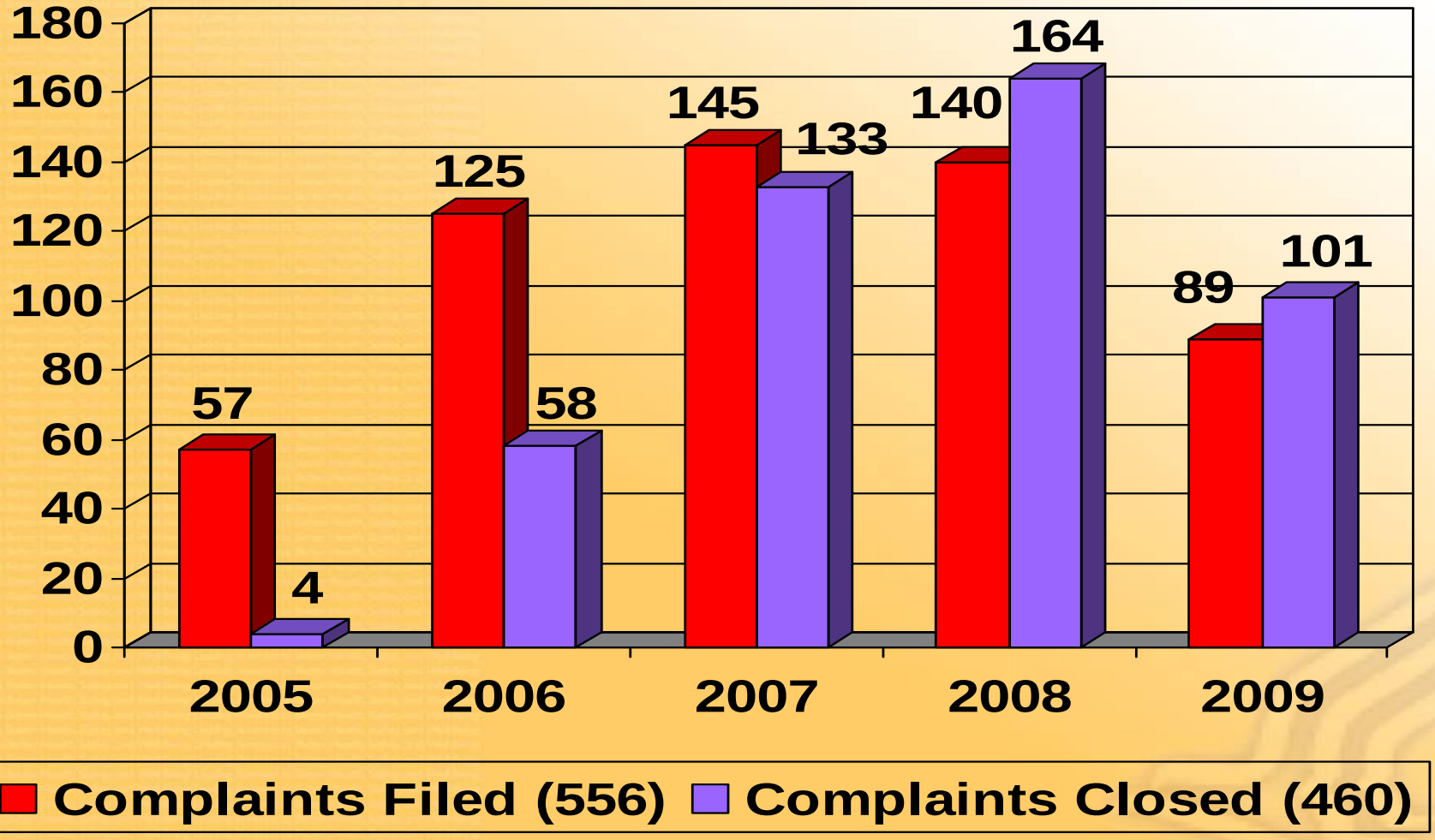
Complaint Investigations

- Every complaint received is reviewed and the allegations are analyzed.
- An investigation is launched when warranted by the facts and circumstances presented.
- OCR investigations have resulted in changes in privacy and information security practices and other corrective actions in over 10,000 cases since April 2003.
- Corrective action obtained by HHS from covered entities has resulted in systemic change

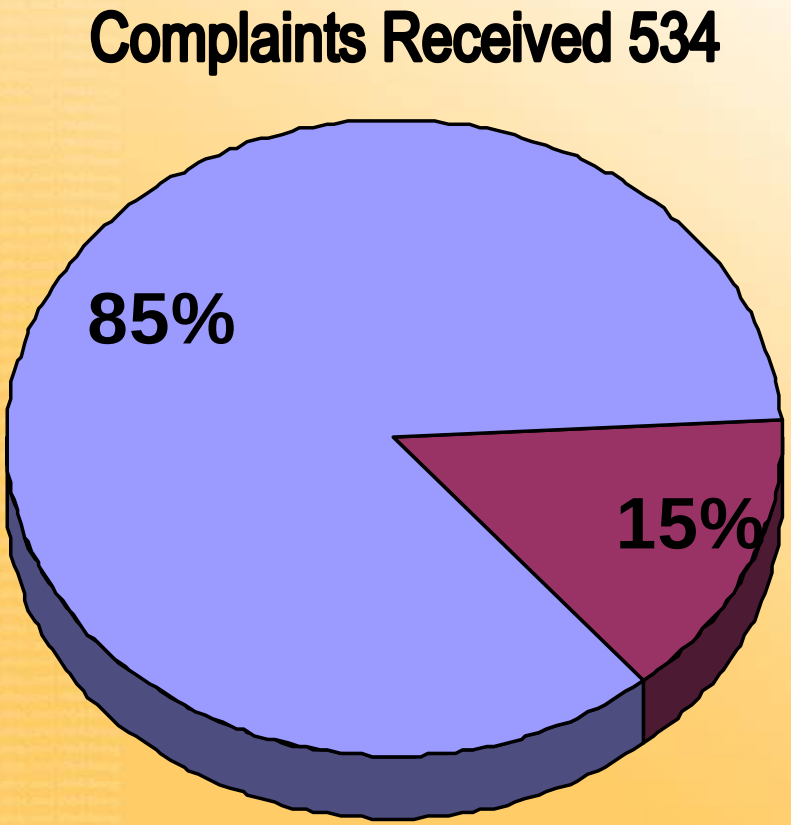
HIPAA Security Rule Enforcement

- Delegation of Authority – July 27, 2009
- Streamline, unify, simplify investigation and resolution of cases
- Address growing overlap of security/privacy in HIT environment
- Support and cooperation of CMS to effectuate transfer of cases, system support, technical experts
- OCR investigative staff in Regional Offices allows expansion of compliance review and on-site investigatory methods

Security Rule Complaints By Year



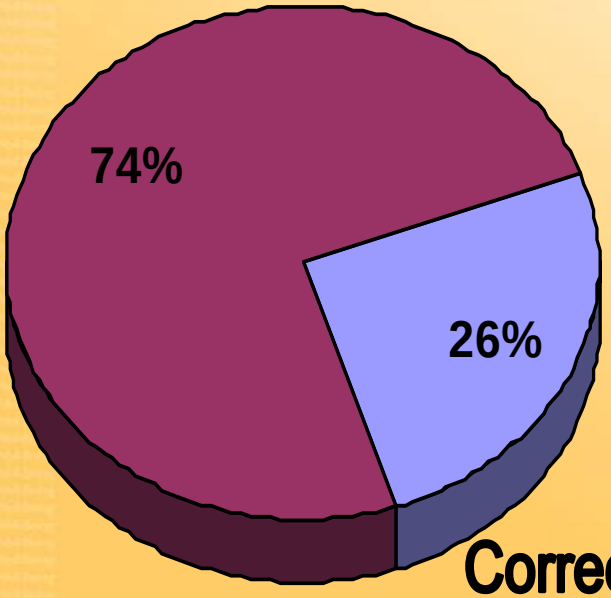
Status of All Security Rule Complaints April 2005 to December 2009



Total Investigated Resolutions
April 2005 to December 2009

Complaints Investigated 129

No Violation 96



Corrective Action Obtained 33

No Violation | Corrective Action Obtained (Change Achieved)

Issues in Security Enforcement Actions

(April 20, 2005 to December 31, 2009)

The compliance issues investigated most frequently, in order, are:

- Information access management
- Access controls
- Security awareness and training
- Security incident procedures
- Device and media controls

Case Example #1

- Electronic storage media containing e-PHI for 2 million individuals were stolen from a vehicle used by a hospital's off-site storage vendor.
- HHS compliance review evaluated CE's overall Security Rule risk management process.
- HHS required the hospital to put into place corrective action plan to appropriately protect e-PHI
  - Encryption of e-PHI placed on storage media
  - Contactor requirements to transport and store backup tapes
  - Security awareness training policies
  - Periodic review and updates of policies and procedures

Case Example #2

- Consumer complained after receiving a letter from a CE reporting the theft of a device that held e-PHI
- HHS determined that a PC had been stolen while a reception desk was left unattended, and that the e-PHI stored on the hard drive was not encrypted.
- CE took corrective actions to improve
  - Physical security safeguards (stronger locks and doors)
  - Retrained its employees on privacy and security policies and procedures, instituting a policy of closing and locking doors when offices were unattended
  - Encrypted the e-PHI stored on electronic devices and other technological safeguards

Case Example #3

- A consumer reported that a CE's e-PHI could be viewed unprotected on the Internet.
- HHS determined that the CE had put into production security patches to server O/S without testing.
- The release had been placed into production for months earlier.
- HHS required the health plan to review and implement
  - Change management process
  - Periodic evaluation of environmental and operational changes affecting the security of e-PHI

Privacy and Security Compliance Reviews Arise From Breach Reports

- OCR opens a review of all breach reports involving >500
- CE should be prepared to respond with:
  - Determination of the root cause of disclosure
  - Identifying gaps in compliance with Privacy and Security Rules that led to the breach
  - Provide evidence that the root cause has been addressed to insure that further breaches do not occur

United States Department of Health & Human Services

Resolution Agreements

Marilou King, J.D.
Civil Rights Division, Office of General Counsel

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.

What is a Resolution Agreement?

- Resolution Agreement and Corrective Action Plan is *not*:
  - A formal finding of facts
  - A formal finding of a violation
  - An admission of a violation
- Resolution Amount is *not* a civil monetary penalty, fine, or other formal penalty.
- Because Resolution Agreement an informal resolution:
  - Covered entity has no right to formal process
  - Covered entity has no right to request an ALJ 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 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

Part of Overall Enforcement Strategy

- RA/CAP is one of several effective enforcement tools, to be used on case by case basis.

- In investigations where there is evidence of significant noncompliance with the Privacy and Security Rules, covered entities may be presented a similar resolution option.

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.