United States Department of Health & Human Services

*Office of the Secretary*
**Office for Civil Rights (OCR)**

# HIPAA Privacy and Security Rules Updates

## *18th National HIPAA Summit*
### *February 3-4, 2010*

***Susan McAndrew, J.D.***
***Deputy Director,***
***Health Information Privacy***

# HIPAA Privacy Rule Updates

- Regulatory Actions 2009
  - Breach Notification Guidance 4/2009
  - Breach Notification IFR 8/2009
  - Enforcement IFR 10/2009
  - GINA NPRM 10/2009
- Regulatory Actions Scheduled for 2010
  - HITECH Privacy & Security Rule, including more Enforcement Rule changes, NPRM/Final
  - Breach Notification Final
  - Breach Guidance Annual Update
  - Accounting for Disclosures from EHRs NPRM
  - GINA Final

# American Recovery and Reinvestment Act of 2009

**Title 13:** Health Information Technology for Economic and Clinical Health Act (HITECH Act)

**Subtitle D:** Privacy (Privacy Rule and Security Rule)

**Section 13402 Breach Notification**

Guidance on Unsecured Protected Health Information

IFR on Notice Requirements for Covered Entities and Business Associates

# Breach Notification
## 45 CFR 164 Subpart D

- HHS Issues RFI – April 2009
  - Guidance on Technologies/Methodologies for unusable, unreadable, indecipherable PHI
- HHS Issues IFR – August 24, 2009
  - Effective for breaches after 9/23/09
  - 60 day public comment period ends 10/23/09
  - Approximately 120 comments received

# Breach Notification IFR

- Covered entities must notify each affected individual of breach of “unsecured protected health information.”
- HHS Breach Notification Guidance: PHI is “unsecured” if it is NOT
  - Encrypted
  - Destroyed
- “Breach” defined as:
  - Impermissible use/disclosure
  - “Compromises privacy/security”
  - Exceptions for inadvertent, harmless mistakes

# Breach Notification IFR

- Business associate must notify covered entity of breach
- Notice to media if more than 500 people affected.
- Notifications to be provided without unreasonable delay (but no later than 60 days) of discovery of breach.
- Notice to Secretary of breach and posting on HHS Website.

# Breach Reports

- Notifications to the Secretary required by web portal
- As of January 2010, 35 reports of breaches affecting 500+ individuals reported, resulting in 712,000 notices
  - Mostly ePHI that is contained in lost or stolen unencrypted media or portable device
- Also received over 300 reports of smaller breaches
  - Mostly paper records sent to wrong fax number, wrong address, wrong individual

# FTC Breach Notification for PHRs

- FTC to regulate similar notice requirements for PHR vendors not subject to HIPAA
  - FTC Notice of Proposed Rulemaking Published April 2009; Request for Public Comment due June 1, 2009
  - FTC Final Rule published August 2009

- HHS and FTC to study and recommend to Congress privacy and security requirements for non-HIPAA PHR vendors and best oversight

# Improved Enforcement

**HITECH Act, Sections 13410 and 13411:**

- Noncompliance Due to Willful Neglect
- Distribution of Certain Civil Monetary Penalties
  - Transfer to OCR for Enforcement
  - Percentages to Harmed Individuals
- Tiered Increases in Civil Monetary Penalties
- Enforcement by State Attorneys General
- Periodic Audits
- Criminal Penalties for Individuals (Employees)

**Other:** Secretary's Delegation of Security Rule Enforcement to OCR – July 27, 2009

# Enforcement Rule IFR

- Section 13410(d) of the HITECH Act
  - Effective February 18, 2009
  - Strengthened HIPAA's CMP Scheme by:
    - Creating tiers of increasing penalty amounts that are associated with categories of culpability
    - Revising Affirmative Defenses
- 74 FR 56123: Enforcement Interim Final Rule with Request for Comments – October 30, 2009
  - Effective November 30, 2009
  - Comments accepted until December 29, 2009
  - Approximately 25 comments received

# CMP Categories

- If “person did not know” or “by exercising reasonable diligence would not have known.”
- If the violation was “due to reasonable cause and not to willful neglect.”
- If the violation is due to willful neglect, and is corrected during 30-day time period.
- If the violation is due to willful neglect, and is not corrected during 30-day time period.

Effective Date: Violations occurring after 2/18/2009

# CMPs Increased

## 45 CFR 160.404 - 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** | **$25,000** | **$1,500,000** |

OCR may reduce a penalty if the failure to comply was due to reasonable cause and not willful neglect, and the penalty would be excessive relative to the noncompliance.

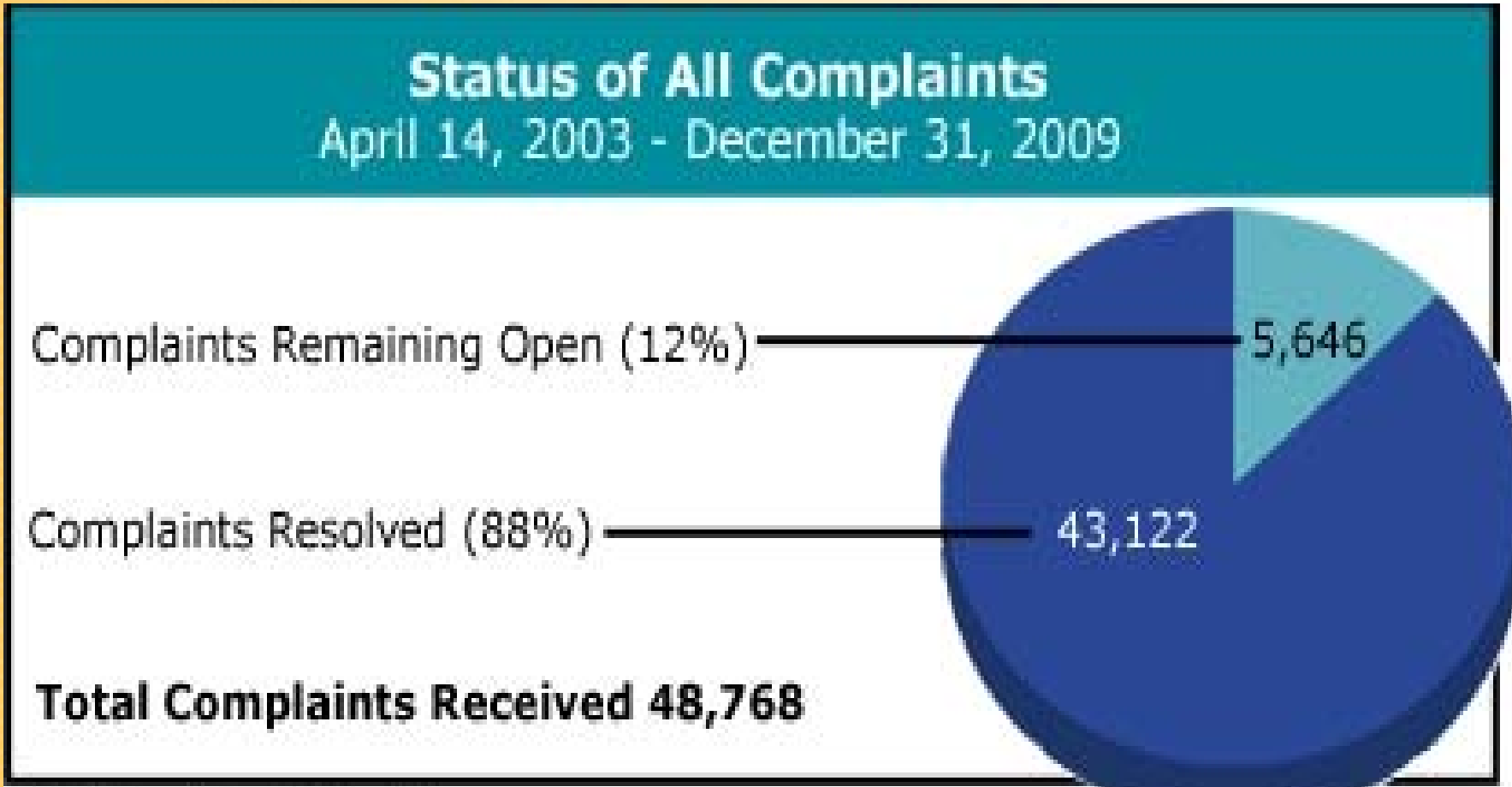
# State Attorney General

- First complaint filed by CT SAG under HITECH authority
- Injunctive relief, statutory penalties sought
- Combination of HIPAA and state law
  - Security Rule violations alleged in loss/theft of portable media
  - Privacy Rule violations alleged in access
  - State law breach notification claims

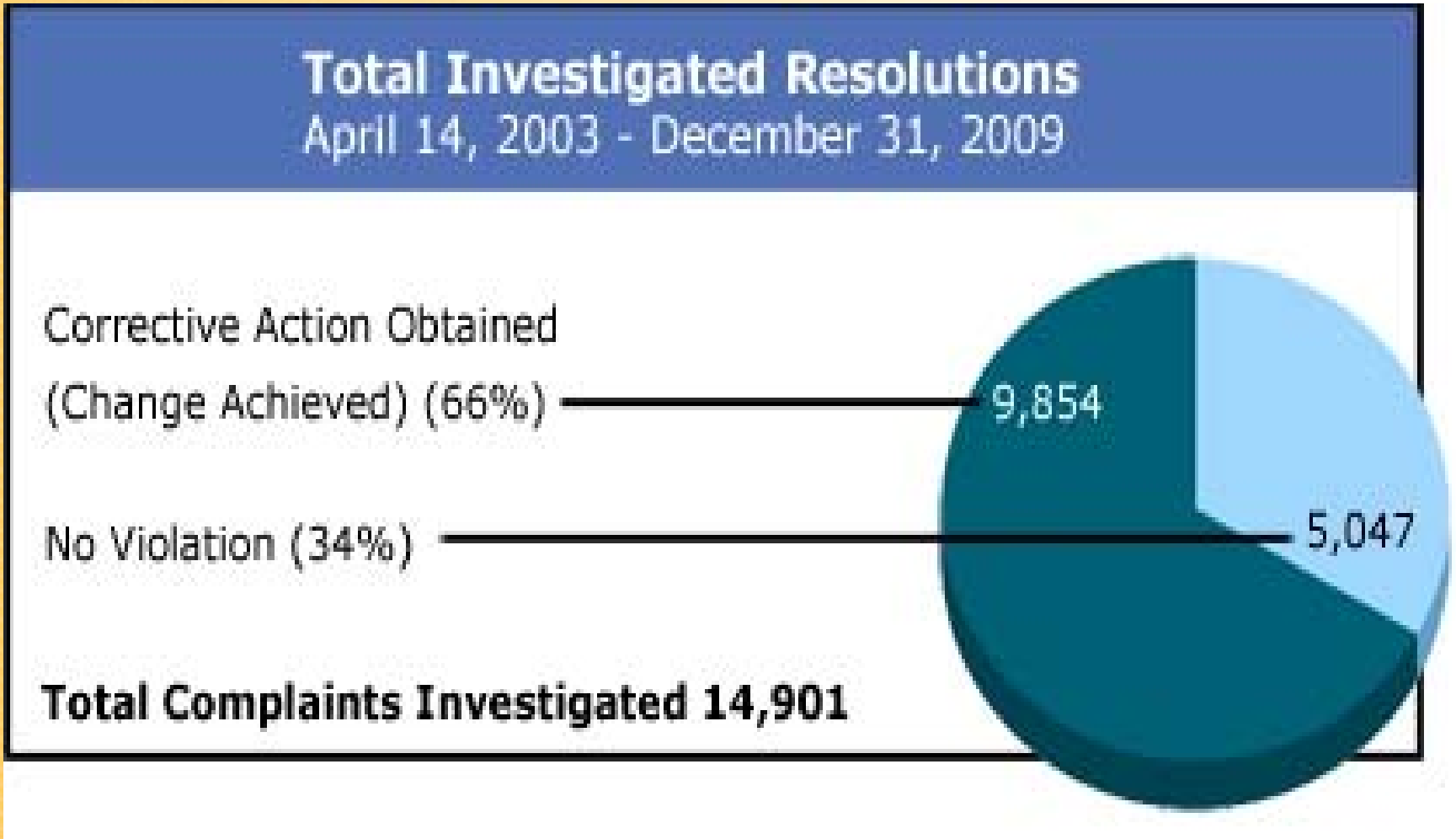
# HIPAA Security Rule

- Delegation of Authority – July 27, 2009
- Streamline, unify, simplify investigation and resolution of cases
- Address growing overlap of security/privacy in HT 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

# Status of All Complaints



# Total Investigated Resolutions



# Genetic Information

- Genetic Information Non-Discrimination Act
  - Signed into law May 21, 2008
  - To protect individuals from discrimination in health insurance and employment on the basis of genetic information
  - Mandates modification of the Privacy Rule to incorporate provisions specific to genetic information
    - Genetic information is protected health information;
    - Prohibit the use or disclosure of genetic information for underwriting

# GINA NPRM

- NPRM issued 10/01/2009
  - Together with IFR for GINA protections from health plan discrimination issued by HHS/CMS, DOL, and Treasury (IRS)
  - EEOC Final Rule for GINA protections from employer discrimination in clearance
- 25 comments received

# HIT HIPAA Privacy Changes

- **Business Associates:** Liable for compliance with Security Rule and uses and disclosures under Privacy Rule; HIEs, certain PHR and others transmitting data are business associates Effective 2/2010
- **Right to Electronic Access:** If covered entity uses an EHR, individual has a right to a copy of his PHI in electronic format. Effective 2/2010
- **Accounting for TPO Disclosures:** If covered entity maintains an electronic health record (EHR), covered entity must include in an accounting disclosures through the EHR for treatment, payment, and health care operations for the three years prior to the request. Effective Date: Depends on CE's adoption of EHR

# Other HIPAA Privacy Changes

- **Right to Restriction:** Covered entity must comply with individual's request for restriction if disclosure: (1) is to health plan for payment or health care operations and (2) pertains to item/service for which provider was paid in full "out-of-pocket." Effective 2/2010
- **Marketing:** Places additional restrictions on covered entity making certain communications about products or services, where entity receives payment in exchange for communication. Effective 2/2010
- **Fundraising:** Covered entity's fundraising communications must provide clear opportunity for individual to opt out of future communications. Effective 2/2010

# Other HIPAA Privacy Changes

- **Minimum Necessary:** Covered entity must limit PHI, to extent practicable, to limited data set, or, if necessary, to minimum necessary. HHS to issue guidance on what constitutes minimum necessary. Effective 2/2010 but sunsets after guidance is issued

- **Sale of PHI:** No direct or indirect remuneration in exchange for PHI, unless the individual signed an authorization; exceptions for public health, research, treatment, sale of business, business associate activities, individual access, and others as determined by Secretary. Effective Date: Regulations required within 18 months after enactment; provisions apply 6 months later.

# Education on Health Information Privacy

- Regional Office Privacy Advisors for education and guidance to covered entities, their business associates and individuals on privacy and security of PHI

- Multi-faceted National Education Initiative on health information privacy to enhance public transparency regarding uses of PHI, including programs to educate individuals about potential uses of their PHI, the effects of such uses, and their privacy rights with respect to such uses

# Studies, Reports and Guidance

- How to best implement the Privacy Rule's requirements for de-identification
  - 2 day workshop in DC on March 8-9
  - Panels of experts and public discussion
  - Web postings with details and materials
- Annual guidance on most effective and appropriate technical safeguards to carry out the HIPAA Security Rule and the HIT Standards adopted under HITECH

# Want More Information?

The OCR website:
http://www.hhs.gov/ocr/privacy/

My contact:
Susan.McAndrew@hhs.gov