United States Department of Health & Human Services

Office of the Secretary
Office for Civil Rights (OCR)

HIPAA Privacy and Security Rules in a HITECH World

17th National HIPAA Summit
September 16, 2009

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

Why HIPAA Matters in a HITECH World

- HIPAA was designed for and applies to electronic information as well as paper; well established baseline for privacy and security
- HIT (in the form of EHRs, PHRs, HIEs or electronic exchanges) presents unique risks and new opportunities
- HITECH builds on HIPAA Privacy and Security Rules to address both risks and opportunities of HIT
- Consumer confidence in privacy and security protections are pivotal to success of eHIE and key to consumer access to the benefits of HIT

American Recovery and Reinvestment Act of 2009

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

  Subtitle A: Promotion of HIT through the Office of the National Coordinator for HIT (ONC)

  Subtitle B: Testing of HIT through the National Institute of Standards and Technology (NIST)

  Subtitle C: Grants and Loan Funding for Incentives for the Use of HIT

  Subtitle D: Privacy (Privacy Rule and Security Rule)

Breach Notification

- HHS Issues RFI – April 2009
  - Guidance on Technologies/Methodologies for unusable, unreadable, indecipherable PHI
  - Comment sought on experience with breach notification laws to inform HHS rulemaking
  - 80 comments received by May 21
- HHS Issues IFR – August 24, 2009
  - Effective for breaches after 9/23/09
  - 60 day public comment period ends 10/23/09

Breach Notification IFR

- Covered entities must notify each affected individual of breach of “unsecured protected health information.”
- HHS Breach Notification Guidance: PHI not “unsecured” if it is
  - Encrypted
  - Destroyed
- “Breach” defined as:
  - Impermissible use/disclosure
  - “Compromises privacy/security” – significant risk of harm
  - 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.

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 (02/2010)

Business Associates

- Applies the HIPAA Security Rule's requirements for administrative, physical, and technical safeguards, policies and procedures, and documentation directly to business associates.
- Provides that a business associate may use or disclose PHI only if such use or disclosure is in accordance with the HIPAA Privacy Rule's required terms for business associate contracts.
- Extends HIPAA's civil and criminal penalties to business associates for violations of these provisions.

Effective Date: 2/2010

Business Associates

- Any entity that provides data transmission of PHI to a covered entity and that requires routine access to PHI (such as Health Information Exchange Organization) or that contracts with a covered entity to provide a PHR is a business associate and must have a business associate agreement with the covered entity.

Effective Date: 2/2010

HIT HIPAA Privacy Changes

- **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.

Improved Enforcement

HITECH Act:

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

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

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

Increase in CMPs

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

- Up to $100 per violation;
- Capped at $25,000/calendar year for multiple violations of an identical requirement or prohibition.

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

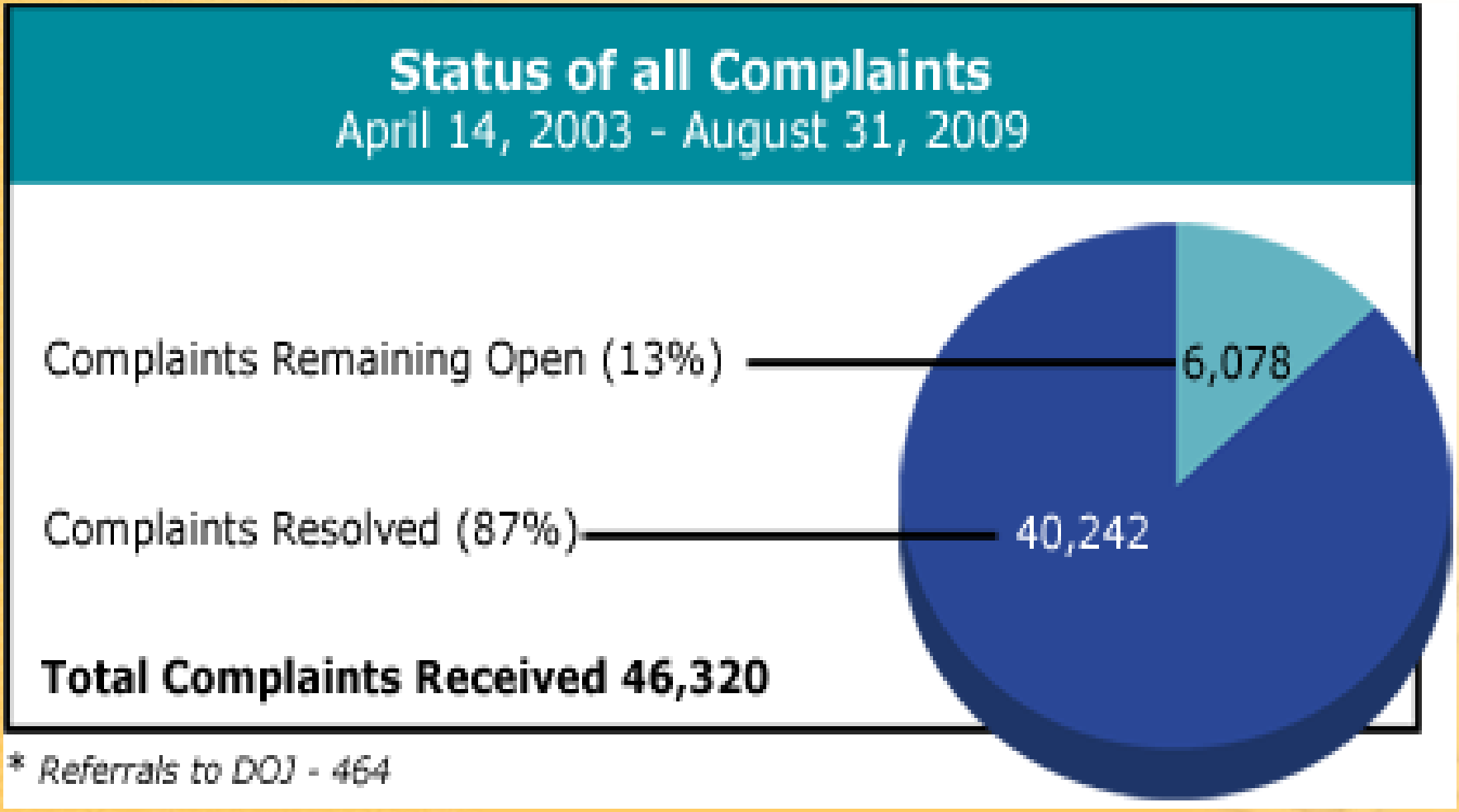
- $100 to $50,000 or more per violation;
- Capped $1.5 million/calendar year for multiple violations of an identical requirement or prohibition.

Effective Date: Violations occurring after 2/18/2009

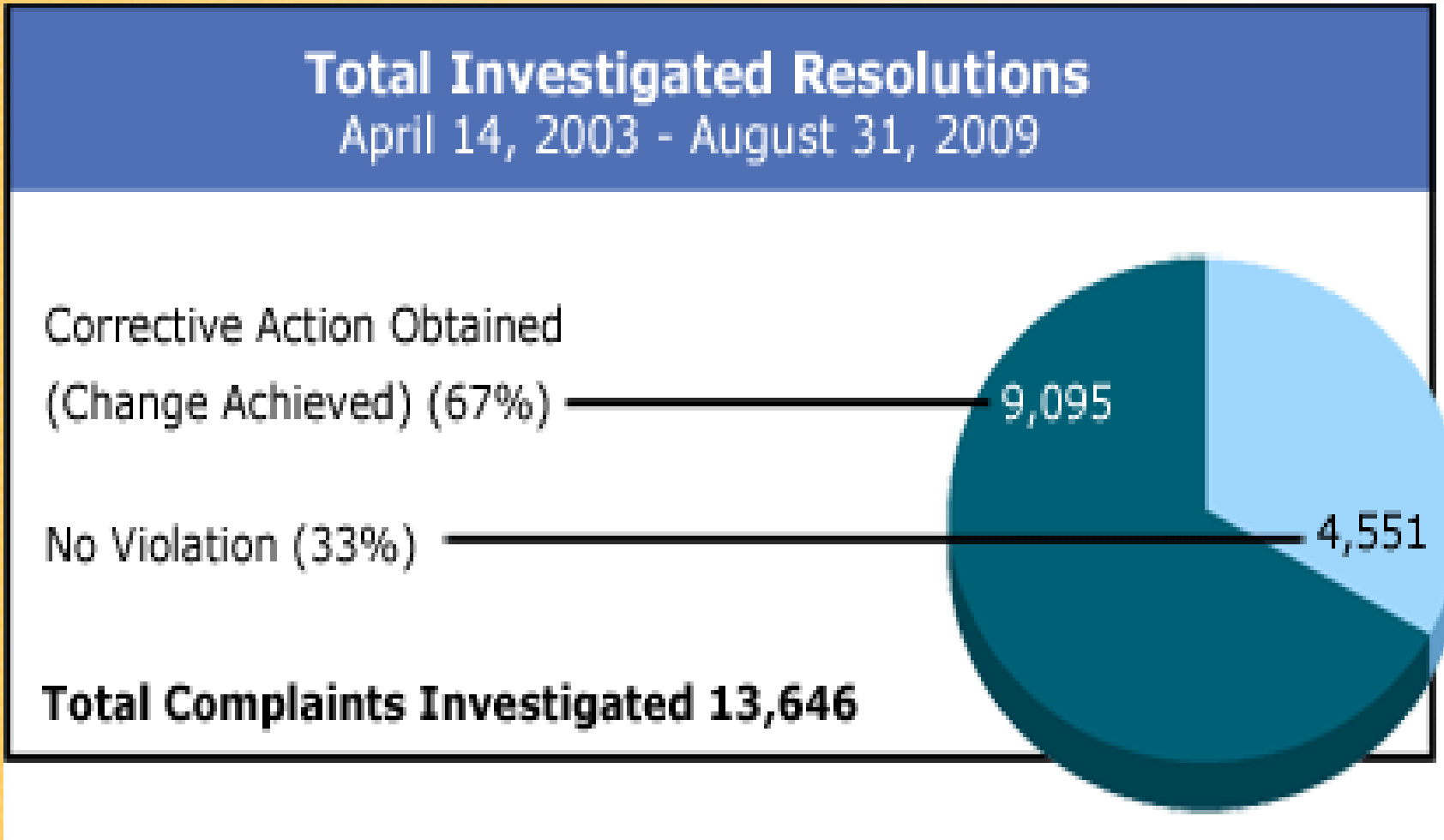
HIPAA Security Rule

- 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



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

- Annual guidance on most effective and appropriate technical safeguards to carry out the HIPAA Security Rule and the HIT Standards adopted under HITECH
- Number and nature of complaints, resolutions, technical assistance, audits and findings and the Secretary's plan going forward
- How to best implement the Privacy Rule's requirements for de-identification
- Definition of "Psychotherapy Notes" and test data that is part of a mental health evaluation

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

Privacy Rule NPRM anticipated in 2009

Want More Information?

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

My contact:
Susan.McAndrew@hhs.gov