United States Department of Health & Human Services

Office of the Secretary
Office for Civil Rights (OCR)

HIPAA Update: Where We Are Today

4th National HIPAA West Summit
October 4-6, 2010

Adam Greene, JD, MPH
Senior Health IT and Privacy Specialist

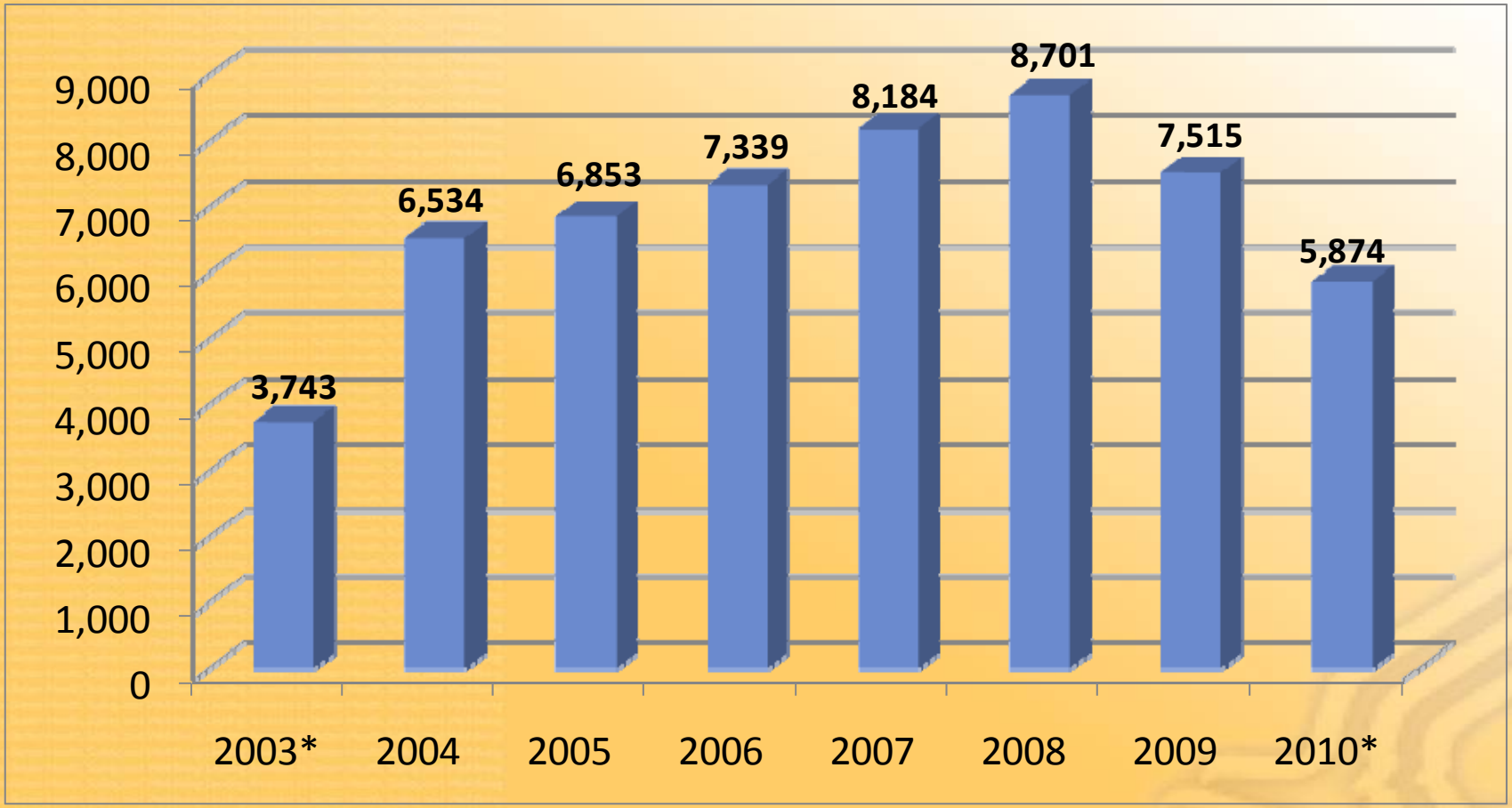
Agenda

- Enforcement Trends
- Current HIPAA Privacy and Security Issues

HIPAA: Then and Now

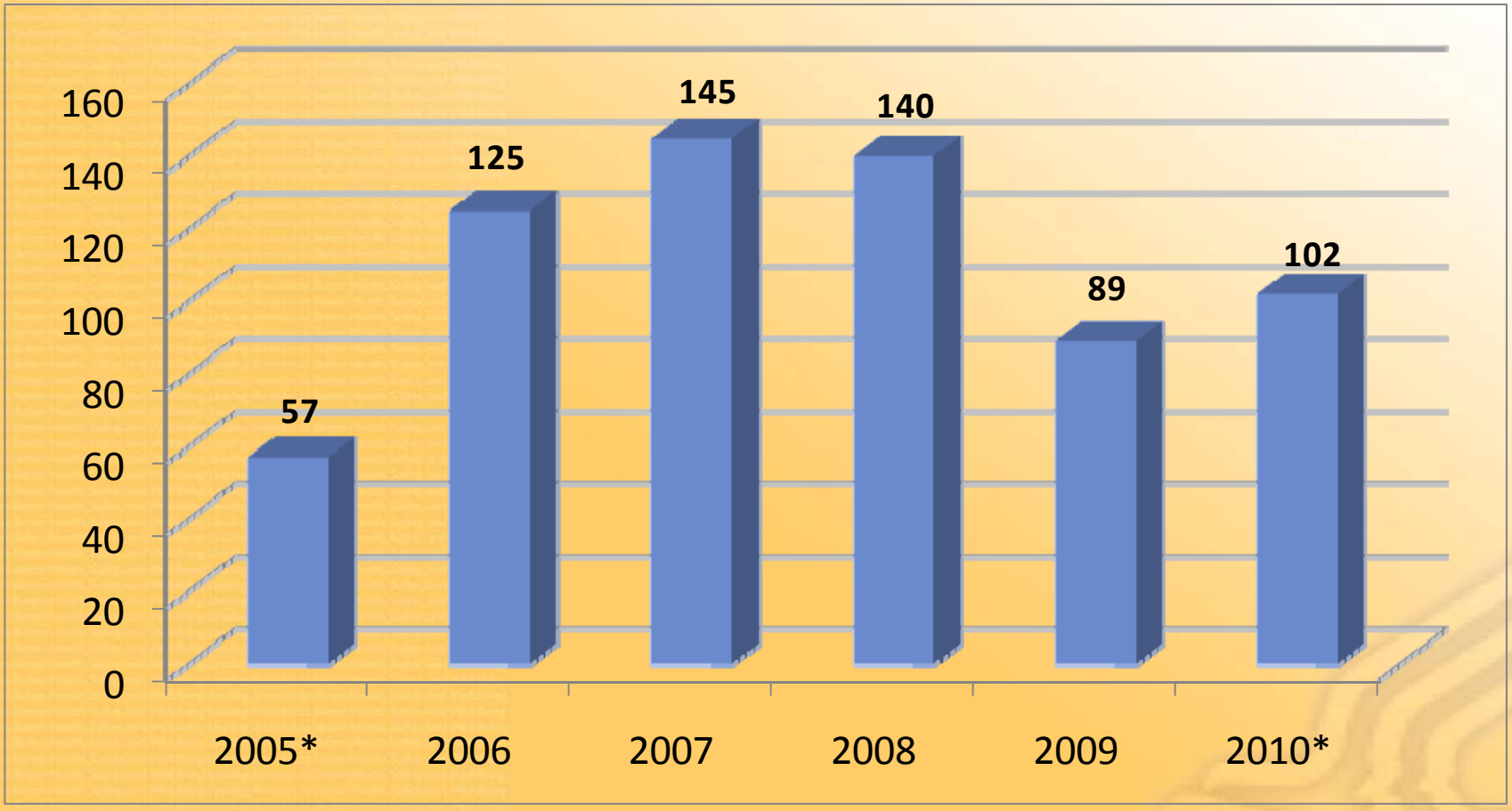
- December 28, 2000 – HIPAA Privacy Rule is finalized

Privacy Complaints Per Year



* Partial year (2010 is through 8/31/10)

Security Complaints Per Year



* Partial year (2010 is through 8/31/10)

Top 5 Privacy Issues

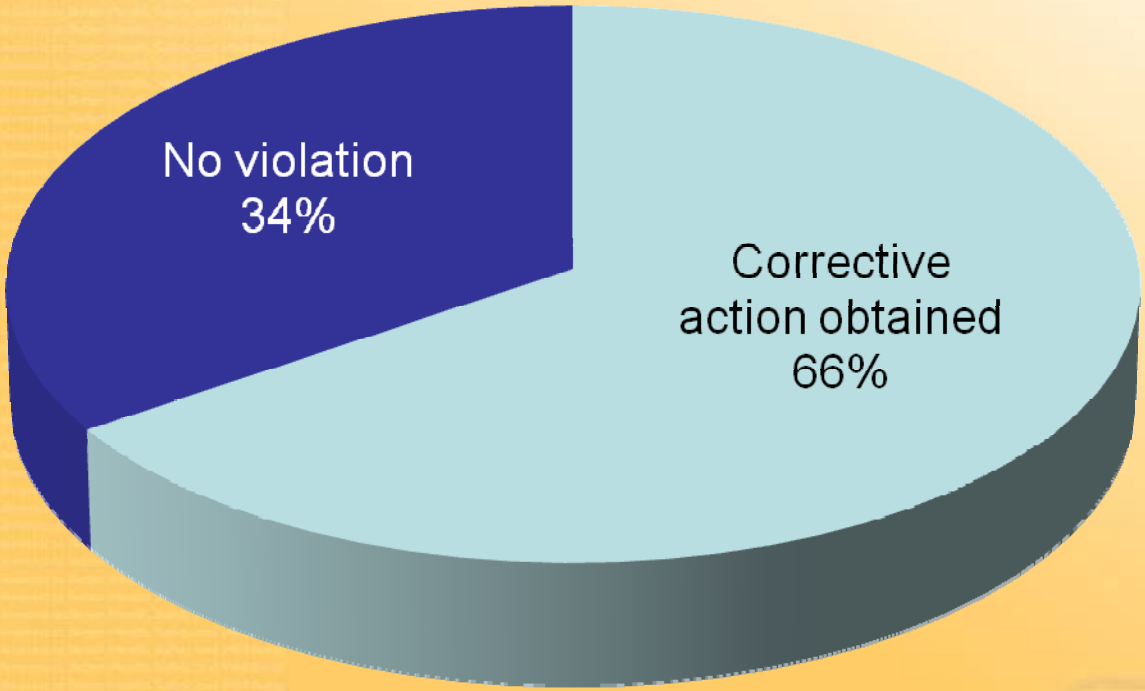
1. Impermissible uses and disclosures
2. Lack of reasonable and appropriate safeguards
3. Failure to provide individual with access to designated record set
4. Failure to use or disclose minimum necessary
5. Inadequate complaint process

Top 5 Security Issues

1. Information access management
2. Access controls
3. Security awareness and training
4. Security incident procedures
5. Device and media controls

Total Investigated Privacy Resolutions

(April 14, 2003 - August 31, 2010)



Resolution Agreements

- Providence Health & Services (July 2008)
  - Loss of electronic backup media and laptop computers
  - 3-year corrective action plan & $100,000
- CVS Pharmacy (January 2009)
  - Improper disposal of records
  - 3-year corrective action plan & $2.25 million
  - External monitor
- Rite Aid Corp. (July 2010)
  - Improper disposal of records
  - 3-year corrective action plan & $1 million
  - External monitor

Increased Penalties

- Pre-HITECH Act
  - $100 per penalty
  - $25,000 annual cap per identical provision
- Post HITECH Act
  - $100 to $50,000 or more per violation
  - $1.5 million annual cap per identical provision

Breach Notification

- Securing PHI
- Monitoring for breaches
  - Reasonable diligence
- Avoiding unreasonable delay
  - Length of investigation
  - Reconstructing data
- Conducting a risk assessment
- Notifying individuals

Electronic Health Records

- Reasonable and appropriate safeguards
  - Encryption
- Minimum necessary
  - How specific should access levels be?
- Patient access and amendment
  - Use of EHR portals
  - Connecting to a PHR

Identifiability of PHI

- Availability of public data sources
- Technological advances
- Genetic information

Health Information Exchange

- Health Information Organization vs. Conduit
  - Routine vs. random and infrequent access
- Personal Health Record Vendors
  - Acting on behalf of a covered entity?
- Changing nature of disclosures
  - Loss of control by covered entities?

Cloud Computing

- Types of cloud computing services
  - Data storage
  - Internet-based applications
  - Internet-based e-mail
- Business associate agreements with cloud computing service providers
- Reasonable and appropriate safeguards
  - Properly configuring settings

Want more information?

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

My contact:
adam.greene@hhs.gov