United States Department of Health & Human Services

Office of the Secretary

Office for Civil Rights (OCR)

The Role of the HIPAA Privacy Rule

CMS/NIST HIPAA Security Rule Conference

May 19, 2009

Marilou King, JD

Acting Senior Advisor for Enforcement

Office for Civil Rights, Health Information Privacy Division

Privacy & Security Rules Overlap

- Concepts of Privacy and Security of PHI inexorably linked
- The Privacy Rule Safeguards standard (§ 164.530(c)) requires a covered entity to safeguard the privacy or confidentiality of all PHI, including paper, oral or EPHI
- The Security Rule General Requirements standard (§ 164.306(a) requires a covered entity to ensure the confidentiality, integrity, and availability of all EPHI the covered entity creates, receives, maintains, or transmits

Example of Violation of Both Rules

- An existing information system with EPHI has no capability to provide access controls and workforce members are able to view more information than needed for their job function. The covered entity did not make a decision whether to implement procedural access controls. No additional safeguards or additional training were implemented.
  - Privacy violation(s): Lack of minimum necessary §164.502(b); No administrative and technical safeguards §164.530(c); No specific privacy training § 164.530(b)
  - Security violation(s): Lack of access controls §164.312(a)(1); No specific security training § 164.308(a)(5)

Example of Violation of Both Rules

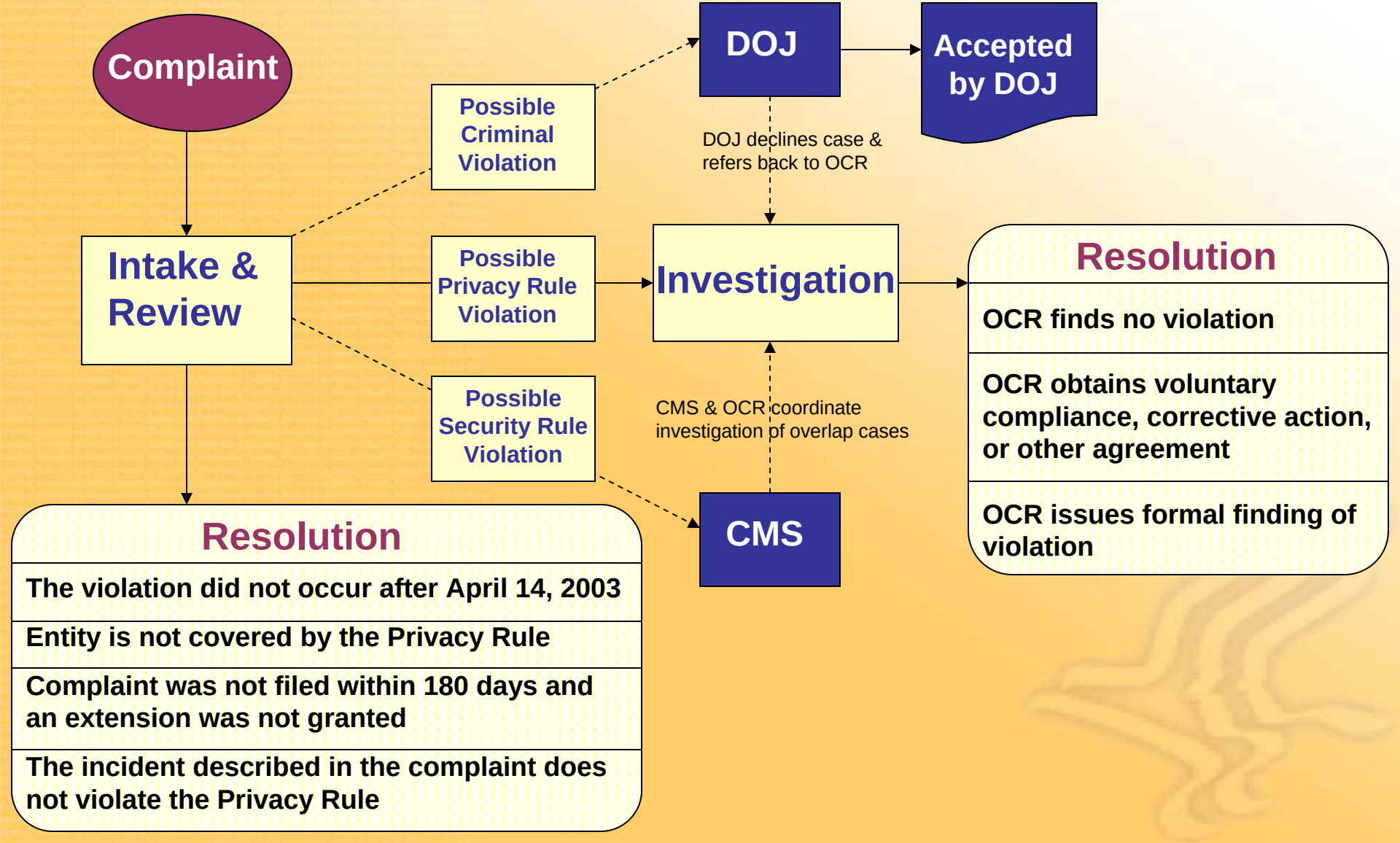
- As part of community outreach and charity efforts a covered entity donates surplus workstations and servers to a special needs school. No procedures for device and media controls including disposal and media re-use were developed by the covered entity. The workstations and servers included PHI that was accessed by staff and volunteers at the school.
  - Privacy violation(s): Lack of administrative and technical safeguards §164.530(c)
  - Security violation(s): Lack of device and media controls policies and procedures §164.310(d)(1)

Privacy Rule Enforcement

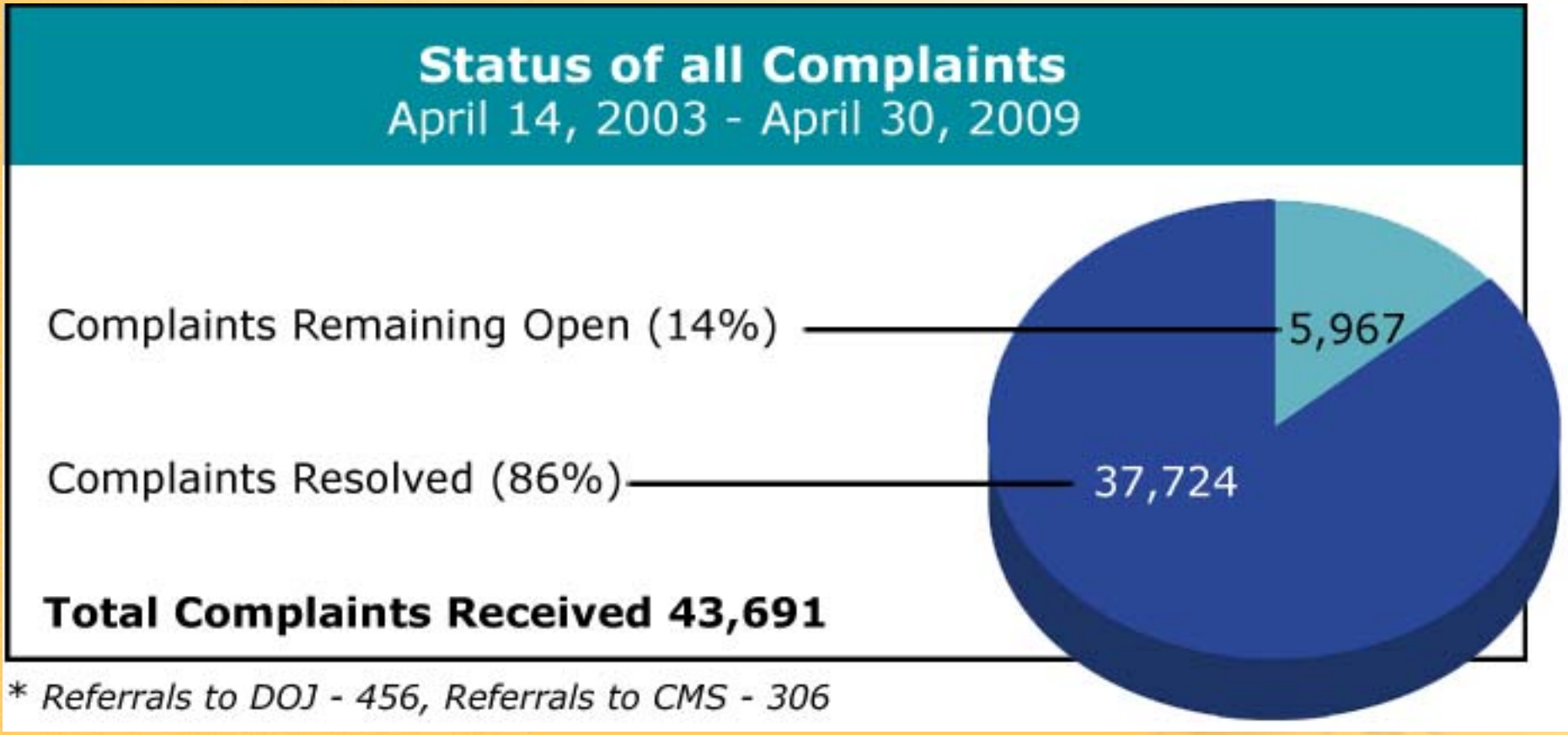
Process and Results

OCR

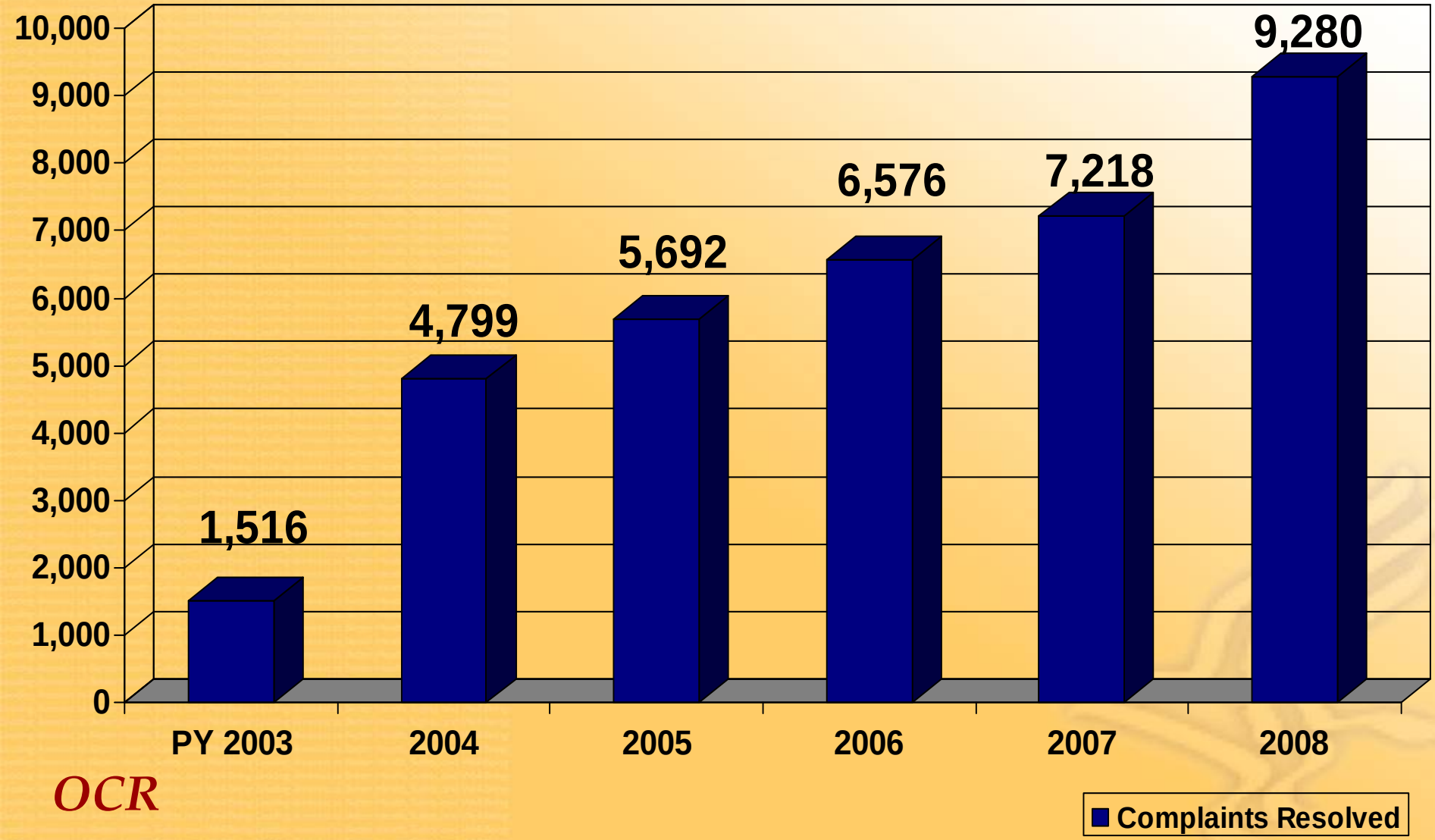
HIPAA Privacy Rule Complaint Process



Pie Chart: All Complaints

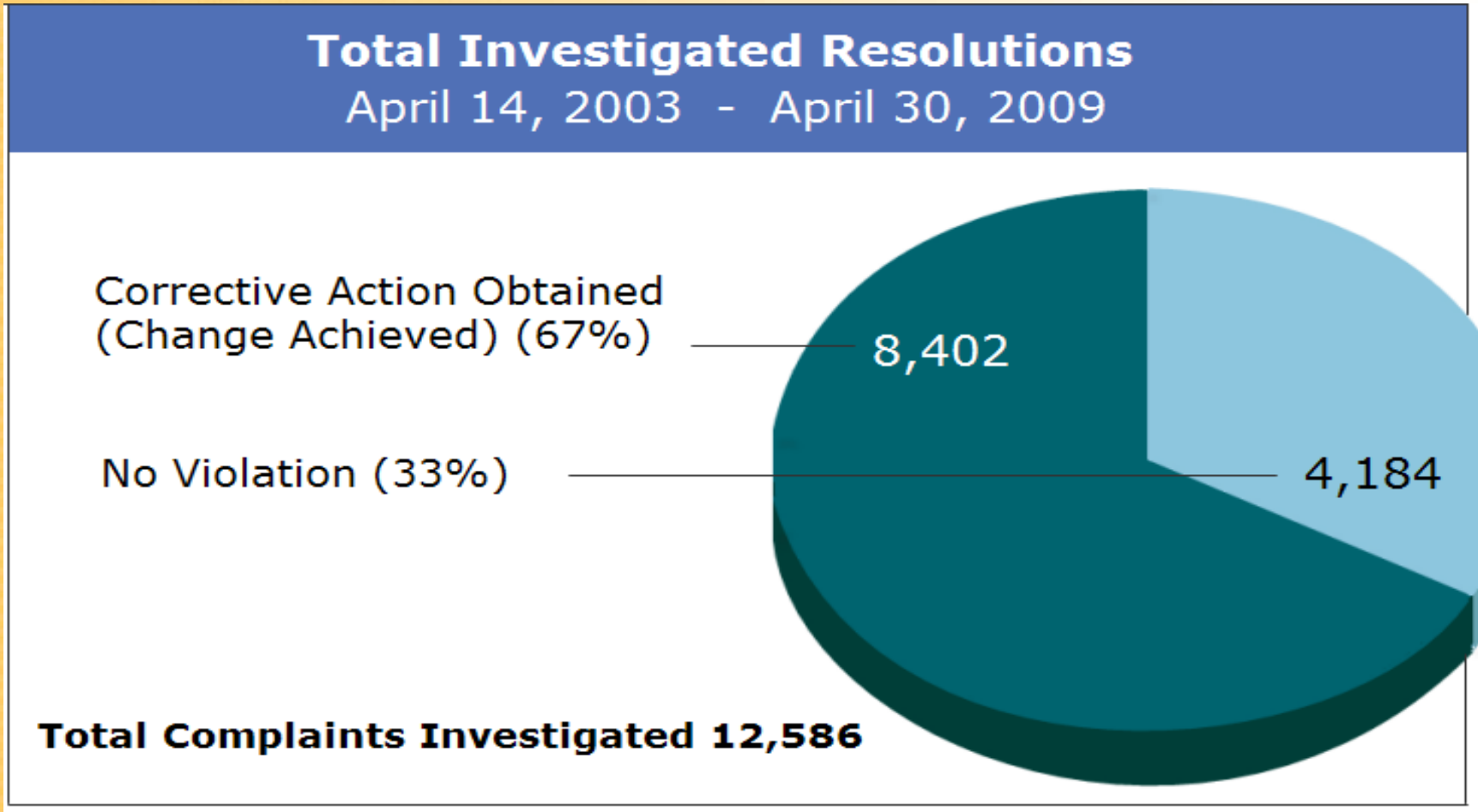


Total Resolutions by Calendar Year

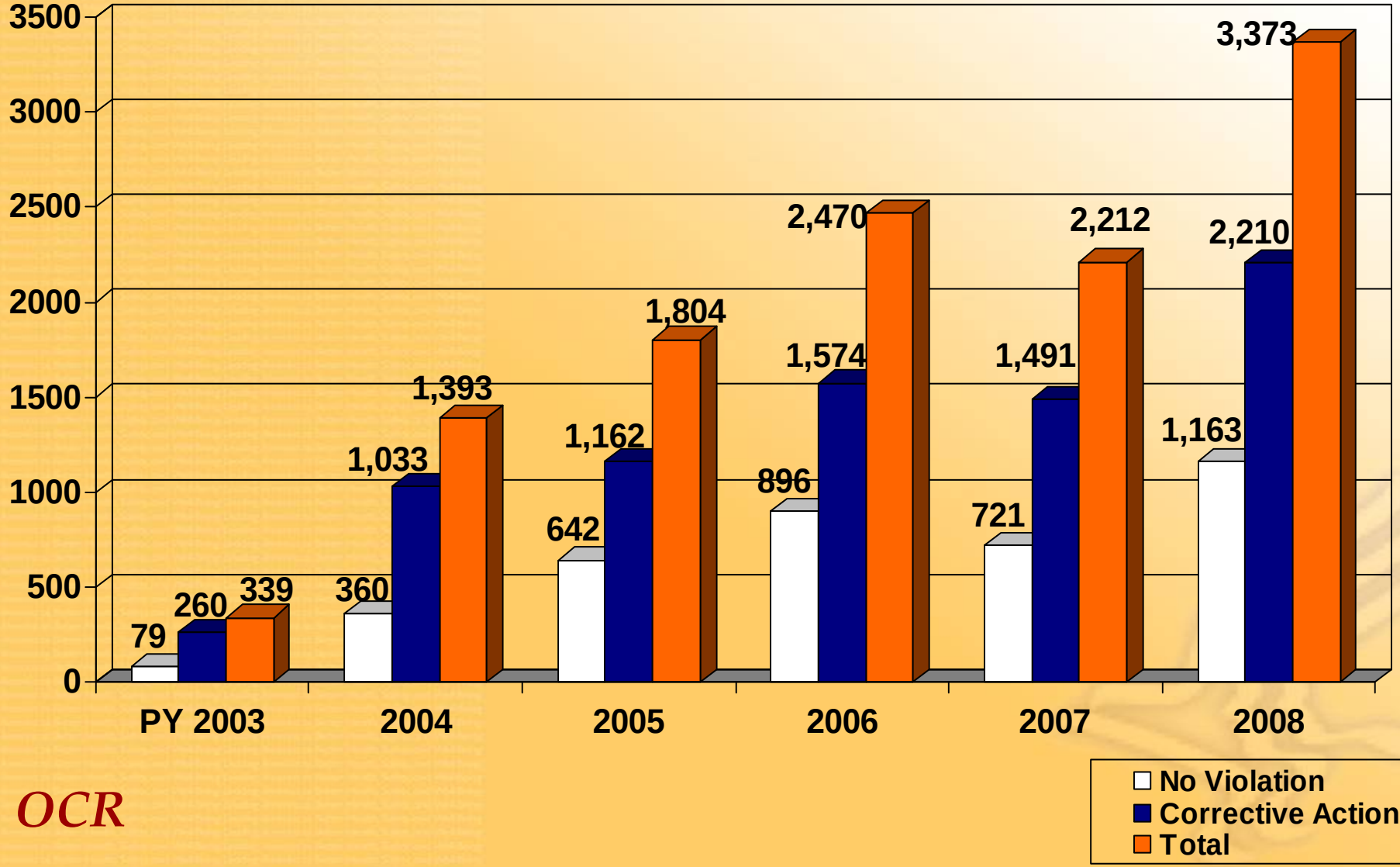


OCR

Pie Chart: Total Investigated



Investigated Resolutions



OCR

Issues in Enforcement Actions

(April 14, 2003 to April 30, 2009)

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

- Impermissible use or disclosure of an individual's identifiable health information
- The lack of adequate safeguards to protect identifiable health information
- Refusal or failure to provide the individual with access to or a copy of his/her records
- The use or disclosure of more than the minimally necessary information
- Failure to have the individual's valid authorization for a disclosure that requires one

CE Types in Enforcement Actions

(April 14, 2003 to April 30, 2009)

The most common types of covered entities that have been required to take corrective actions and voluntarily comply, in order of frequency, are:

- Private physician practices
- General hospitals
- Outpatient facilities
- Health plans (Group Health Plans and Health Insurance Issuers)
- Pharmacies

Providence Resolution Agreement

- Health care system based in Seattle, Washington
- Series of five incidents occurring between September 2005 and March 2006
- Incidents giving rise to the agreement involved two entities within the system
  - Providence Home and Community Services and
  - Providence Hospice and Home Care

Providence Investigation

- Triggered by 31 complaints submitted to OCR and CMS
- Complaints merged into joint compliance reviews by CMS and OCR
- Practices of entities created vulnerabilities that led to massive losses of PHI
- Cooperation of Providence
- Settled with OCR through Resolution Agreement and Corrective Action Plan on July 16, 2008

Indications of Noncompliance Cited in Resolution Agreement

- Electronic information was not encrypted or otherwise properly safeguarded
- Backup tapes, optical disks, and laptops, all containing unencrypted electronic PHI, were removed from the Providence premises and left unattended in vehicles
- Media & laptops were ultimately lost or stolen, compromising the PHI of over 386,000 patients
- Management knew of such practices but allowed it to continue

Actions to Settle Cases

- $100,000 resolution amount
- Corrective Action Plan

1. Revise policies, procedures
   - New risk assessment and risk management
   - Improved physical & technical safeguards (e.g., encryption) for off-site transport and storage of electronic media containing patient information
   - Subject to HHS approval
2. Train workforce members on safeguards
3. Conduct audits and site visits of facilities
4. Submit implementation report and annual reports to HHS for period of three years

Lessons Learned

- Effective compliance means more than just written policies and procedures
- Covered entities need to continuously monitor implementation
- HHS willing to work with cooperative entities to implement effective changes to ensure that consumers are protected
- Covered entities need to ensure that these efforts include
  - Effective privacy and security staffing
  - Employee training
  - Physical and technical features

CVS Investigation

- Compliance Review of all CVS retail pharmacy policies and practices related to disposal of PHI
- Conducted jointly with the FTC
- CVS cooperated during investigation
- Settled with OCR through Resolution Agreement and Corrective Action Plan on January 16, 2009
  - Agreement with HHS included payment of $2.25 million
- Simultaneously settled with FTC through Consent Order

Lessons Learned

- Disposal of PHI in unsecured dumpsters or similar repositories is not compliant with safeguards standard of the Privacy Rule
- Personnel involved in disposal must be trained in how to implement disposal safeguards
- Management must supervise implementation

Note - See FAQs on Disposal of PHI

HIT and HIPAA Privacy

The Privacy Rule as a Facilitator Not Obstacle

- Standards reflect many hard choices - which balance the importance of privacy with the need for information in a health care setting
- Narrows the privacy debate to new areas of risk and opportunities for consumers
- Flexibility allows the existing standards to adapt to HIT needs without lowering the baseline of privacy protections and individual rights

OCR's HIT Guidance

- Privacy Rule as a foundation for e-health information exchange
- Privacy Rule provides flexibility to accommodate covered entities' utilization of HIOs and networked environments
- Through the Privacy Rule's business associate provisions a CE can utilize a HIO to provide services or functions on its behalf
  - BA agreement must establish the permitted and required uses and disclosures of PHI by the business associate but may not authorize the business associate to use or disclose PHI in a manner that would violate the Privacy Rule.
  - Contract also must require the business associate to appropriately safeguard PHI.

Privacy and Security Framework

- Privacy and Security Framework
  - Correction Principle and FAQs
  - Openness and Transparency Principle and FAQs
  - Individual Choice Principle Privacy and Security Framework: Collection, Use, and Disclosure Limitation Principle and FAQs
  - Safeguards Principle and FAQs
  - Accountability Principle and FAQs

- The HIPAA Privacy Rule's Right of Access and Health Information Technology
- Personal Health Records (PHRs) and the HIPAA Privacy Rule

OCR Web Site

- http://www.hhs.gov/ocr/hipaa/
- Additional guidance & resource materials
  - Health Information Technology (HIT)
    - http://hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/index.html
  - Frequently Asked Questions About the Disposal of Protected Health Information
    - http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf