United States Department of Health & Human Services

Office of the Secretary
Office for Civil Rights (OCR)

Enforcement and Policy Challenges in Health Information Privacy

Linda Sanches
HIPAA Summit Special Edition
December 14, 2007

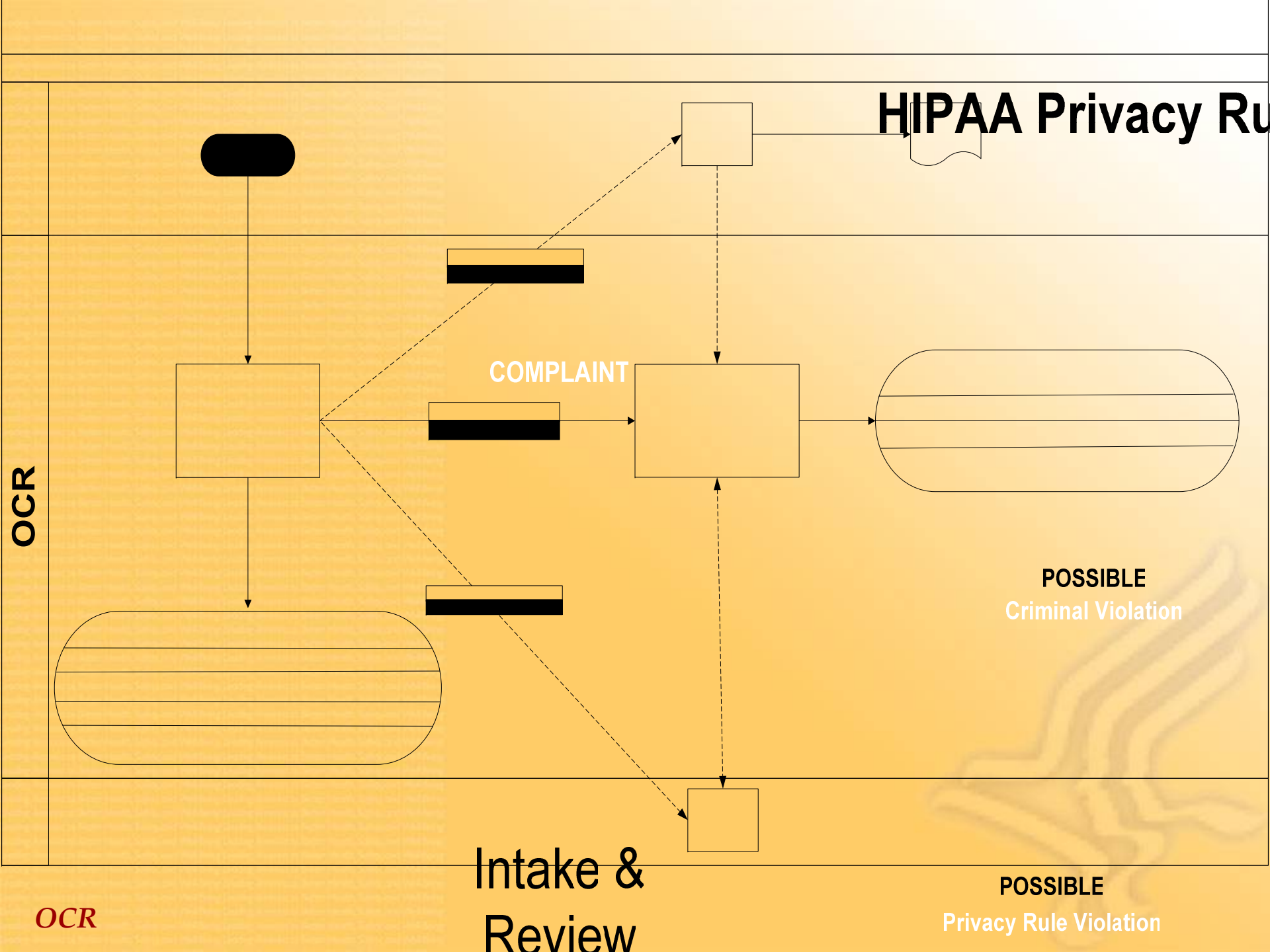
Topics

- Privacy Rule enforcement

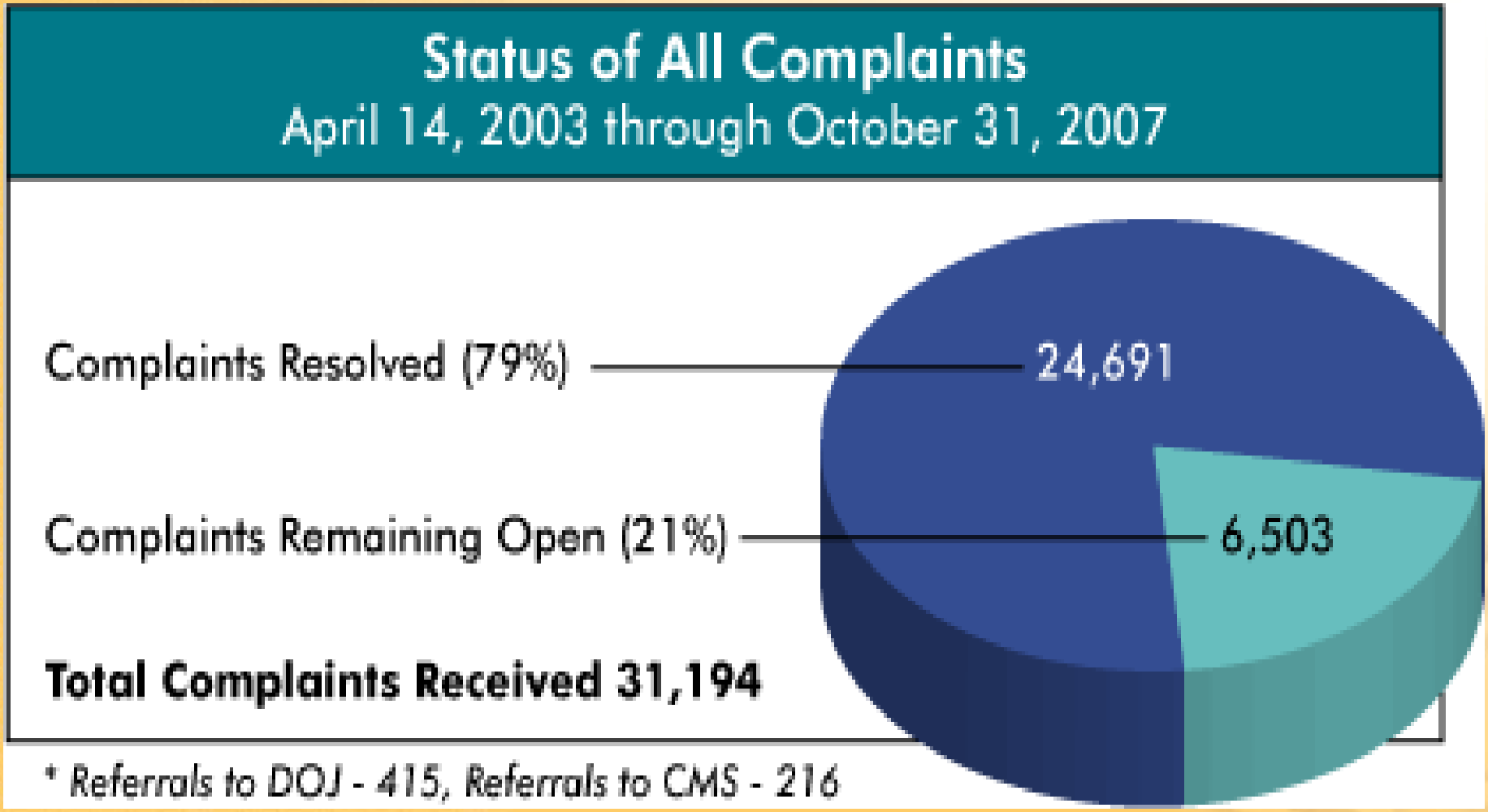
- Other challenges
  - Nationwide Health Information Network
  - Protecting Genetic Information
  - Patient Safety Act
  - Emergency Preparedness
  - Technical Assistance

Complaint Investigations

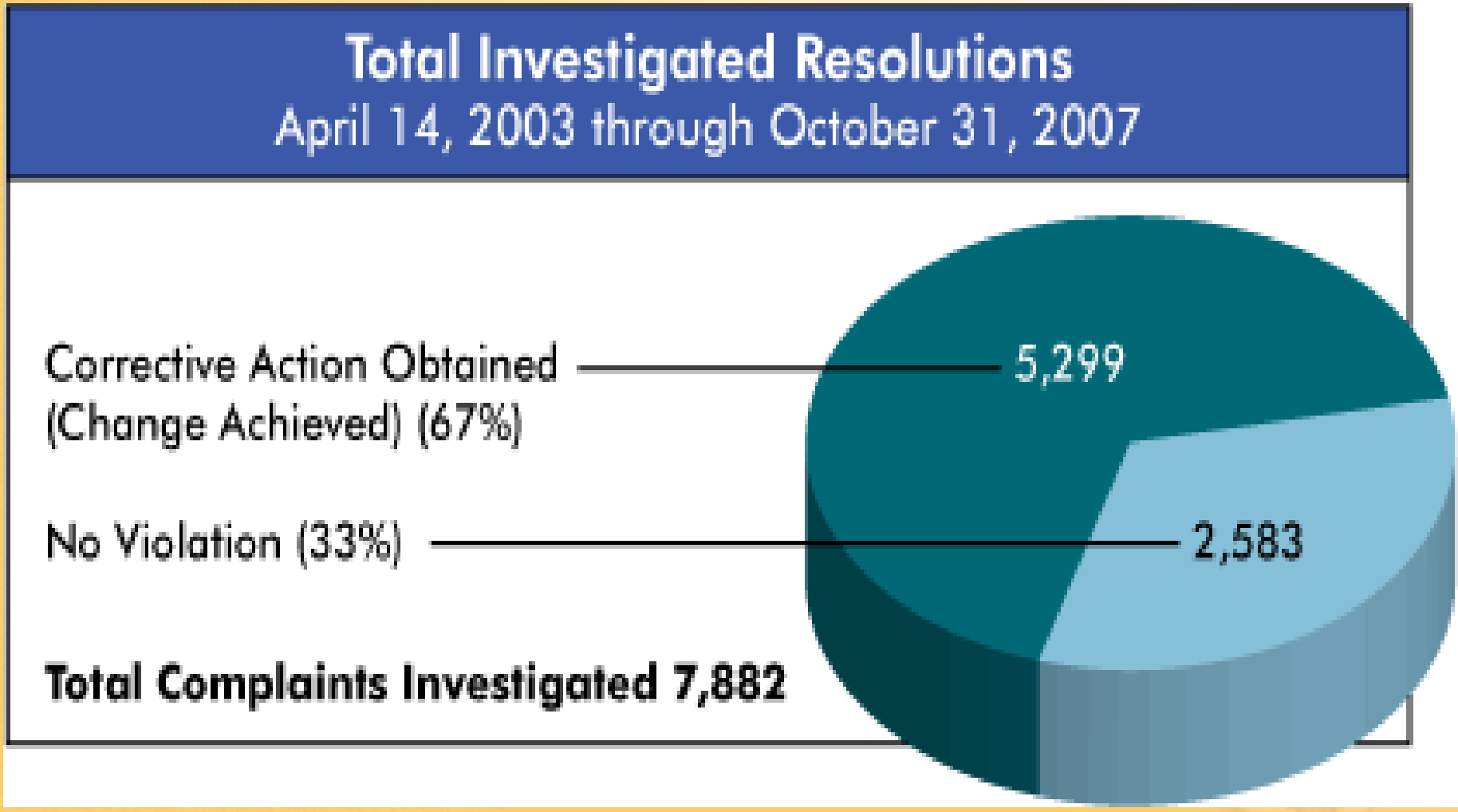
- Every complaint received by OCR is reviewed
- An investigation is conducted where warranted by the facts and circumstances presented by the complaint
- Privacy investigations have resulted in changes in privacy practices and other corrective actions in over 5,299 cases since April 2003
- Corrective action obtained by HHS from covered entities has resulted in systemic change that affects all the individuals they serve


HIPAA Privacy Ru
OCR
COMPLAINT
POSSIBLE
Criminal Violation
Intake &
Review
POSSIBLE
Privacy Rule Violation
OCR

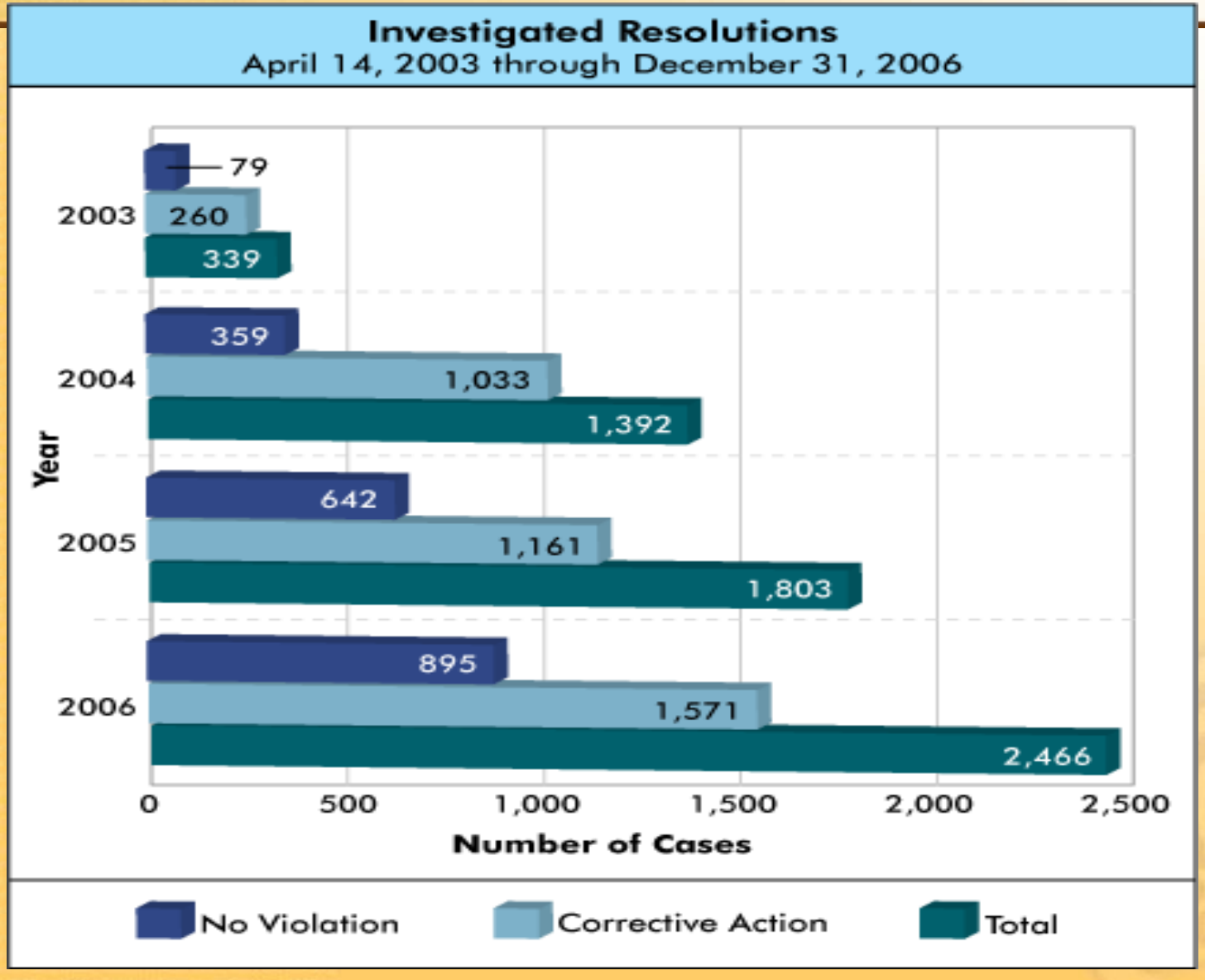
Pie Chart: All Complaints



Pie Chart: Total Investigated



Investigated Resolutions



OCR

Issues in Enforcement Actions

(April 14, 2003 to October 31, 2007)

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 disclosure of more information than is minimally necessary to satisfy a particular request for information
- Failure to have the individual's valid authorization for a disclosure that requires one

Covered Entities in Enforcement Actions

(April 14, 2003 to October 31, 2007)

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

Case Example

- An employee of a major health insurer impermissibly disclosed the protected health information of one of its members without following the insurer's authorization and verification procedures.
- Among other corrective actions to resolve the specific issues in the case, OCR required the health insurer to
  - train its staff on the applicable policies and procedures and to
  - mitigate the harm to the individual
  - apply sanctions to employee who made the disclosure

Case Example (2)

- A national health maintenance organization sent explanation of benefits (EOB) by mail to a complainant's unauthorized family member. OCR's investigation determined that a flaw in the health plan's computer system put the protected health information of approximately 2,000 families at risk of disclosure in violation of the Rule.

- Among the corrective actions required to resolve this case, OCR required the insurer to
  - correct the flaw in its computer system,
  - review all transactions for a six month period and
  - correct all corrupted patient information.

Other Avenues of Enforcement

- The Department has other enforcement tools, such as resolution agreements and imposition of civil money penalties (CMP's), which it will use in appropriate cases

- HHS also obtains privacy compliance through outreach and education efforts

- OCR has reached hundreds of thousands of covered entities and consumers through educational conferences, a toll-free call line, and an interactive website

Other Challenges

Nationwide Health Information Network

- Privacy and Security Are Integral to NHIN
  - Necessary for Public Trust
  - Public Participation Is Engine for Adoption
- HIPAA Levels Playing Field
  - Nationally Accepted Standards for Privacy and Security Already in Place
  - Uniform National Baseline of Protection – More Is Still Good

NHIN & Privacy

- HIPAA Privacy Rule as Facilitator – Not Obstacle to Health IT adoption
  - Standards Reflect Many Hard Choices Balancing Privacy and Access in Healthcare Setting
  - Narrows Privacy Debate to New Areas of Risk and Opportunity for Consumers
  - Flexibility Allows Rules to Adapt to HIE Needs without Lowering Baseline for All
- Personal Health Record (PHR) Good Illustration for Assessing New Risks and Opportunities

Opportunities for PHR

- Personal Health Record (PHR) = Opportunities for the Consumer to Engage in NHIN and Take Advantage of Health IT
  - 24/7 Access to Their Health Information
  - Ability to Migrate Information into PHR to Create a Longitudinal Health Record
  - Ability to Consolidate Health Information from Multiple Providers to Better Manage Their Own Care
  - Capability to Control Access by Others
- Requires Interoperable, Portable, Secure PHR

Gaps for Privacy & NHIN

- Accountability
  - New Players Typically Not Covered by HIPAA
    - Certain Health Care Providers
    - Providers of Network Services
    - Providers of Data Management Services
    - Providers of PHR Services
  - Can Business Associate Contracts Work and Provide Adequate Accountability in the NHIN?

Gaps for Privacy & NHIN

- Uniformity – How Much Is Really Needed
  - Preemption
    - Harmonizing Federal and State Laws
    - Ex: Consents
  - "Flexible and Scalable" Standards
    - Harmonizing Business Practices
    - Example: Minimum Necessary
  - Privacy and Security Solutions for Interoperable Health Information Exchange
    - Looking for Answers

Genetic Information

- HHS Personalized Health Care Initiative
  - Creating privacy foundation for genomic research to advance gene based medicine & health care
  - American Health Information Community working on recommendations for genetic info on EHR
    - Subgroup on privacy and confidentiality
- Genetic Information Non-Discrimination Act
  - To protect individuals from discrimination in health insurance and employment on the basis of genetic information

Patient Safety and Quality Improvement Act

- Establishes voluntary reporting system to enhance the data available to assess and resolve patient safety and quality issues
- Provides Federal privilege & confidentiality protections for "patient safety work product”
- OCR to enforce confidentiality provisions
- In close coordination with AHRQ, OCR will develop and operate the Act's enforcement program

Emergency Preparedness

- Emergency preparedness and recovery planners are interested in the availability of protected health information (PHI)
  - Disasters and emergencies
  - National Disaster Medical System
  - Pandemic and All-Hazards Preparedness Act implementation
- The HIPAA Privacy Rule permits covered entities to disclose PHI for a variety of public health and other purposes
  - OCR providing technical assistance
    - Web tool addresses avenues of information flow that could apply to emergency preparedness activities

Getting out the message

- Targeting outreach
- Assisting entities with compliance through technical assistance
- Informing the public about how the Privacy Rule applies in emerging issues

Other Program Challenges

- Strategic management of enforcement portfolio
- Policy development—balanced & workable Rule

OCR Web Site

- http://www.hhs.gov/ocr/hipaa/
- Privacy Rule text & summary
- Covered entity "decision tool"
- Over 200 frequently asked questions
- Fact sheets
- Information about the OCR enforcement program