United States Department of Health & Human Services

Office of the Secretary
Office for Civil Rights (OCR)

Conducting HIPAA Investigations:

An Office for Civil Rights Perspective

IHS Annual Conference
March 24-25, 2010

Velveta Golightly-Howell, Regional Manager, OCR Region VIII
Roosevelt Freeman, Regional Manager, OCR Region IV

OCR Enforcement

- OCR enforces:
  - traditional civil rights laws
  - Privacy and Security Rules
- OCR enforces these laws through:
  - Complaint investigations
  - Compliance reviews
  - Technical assistance

Office of the Secretary
Office for Civil Rights (OCR)

Georgina Verdugo
Director
U.S Department of Health and Human Services
Office for Civil Rights

Robinsue Frohboese
Principal Deputy Director
U.S Department of Health and Human Services
Office for Civil Rights

Susan McAndrew
Deputy Director, Privacy
U.S Department of Health and Human Services
Office for Civil Rights

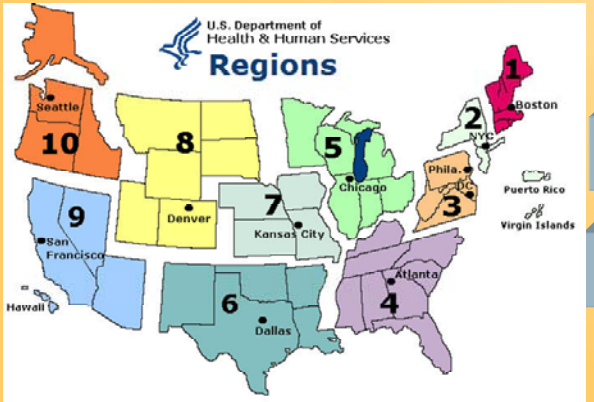
Joanne Chiedi
Deputy Director, Management Operations
U.S Department of Health and Human Services
Office for Civil Rights

Tamara Miller
Deputy Director, Civil Rights
U.S Department of Health and Human Services
Office for Civil Rights

Velveta Howell/Regional Manager
Region VIII—CO, MT, ND, SD, UT, WY

Valerie Morgan-Alston/Regional Manager
Region V—IL, IN, MI, MN, OH, WI

Linda Yuu Connor/Regional Manager
Region X—AK, ID, OR, WA



Peter Chan/Regional Manager
Region I—CT, ME, MA, NH, RI, VT

Michael Carter/Regional Manager
Region II—NJ, NY, PR, VI

Michael Kruley/Regional Manager
Region IX—AS, AZ, CA, GU, HI, NV

Paul Cushing/Regional Manager
Region III—DE, DC, MD, PA, VA,

Roosevelt Freeman/Regional Manager
Region IV—AL, FL, GA, KY, MS, NC, SC, TN

Frank Campbell/Regional Manager
Region VII—IA, KS, MO, NE

Ralph Rouse/Regional Manager
Region VI—AR, LA, NM, OK, TX

Legislative History

- Health Insurance Portability and Accountability Act of 1996 ("HIPAA")
- Subtitle F—Administrative Simplification
- Encourages development of (electronic) health information technologies (transactions)
- Promotes easier information-sharing—security and privacy

HIPAA in HHS

- OCR (the Privacy Rule):
  - Sets Policy through regulations and interpretations
  - Promotes voluntary compliance
  - Enforces through informal resolution and formal enforcement (CMPs)
- Centers for Medicare and Medicaid Services, Office of E-Health Standards and Services (other Administrative Simplification Rules):
  - Security Rule
  - Transactions and code sets
  - Provider and plan identifiers

Scope: Who is Covered?

- Limited by HIPAA to:
  - Health care providers who transmit health information electronically in connection with a transaction for which there is a HIPAA standard
  - Health plans
  - Health care clearinghouses
- Business Associate Relationships

§160.103

Business Associates

- Agents, contractors, and others hired to do the work of, or to work for, the covered entity (CE), and such work requires the use or disclosure of protected health information ("PHI," see next slide).
- The Privacy Rule requires "satisfactory assurance," which usually takes the form of a contract, that a BA will safeguard the PHI, and limit its use and disclosure.

§160.103

Scope: What is Covered?

- Protected Health Information ("PHI"):
  - Individually identifiable health information
  - Transmitted or maintained in any form or medium
- Held or transmitted by CE or their Business Associates
- Not PHI:
  - De-identified information
  - Employment records
  - FERPA records

§160.103

Uses and Disclosures: Key Points

- No use or disclosure of PHI unless permitted or required by the Privacy Rule.
- *Required* Disclosures:
  - To the individual who is the subject of the PHI.
  - To the Secretary of HHS in order to determine compliance.
- All other uses and disclosures in the Privacy Rule are *permissive*.
- Covered Entities may provide greater protections.

Permissive Uses and Disclosures

- To the individual or personal representative
- For treatment, payment, and health care operations (TPO)
- With the opportunity to agree or object
- For specific public priorities
- "Incident to"
- Limited data sets
- As authorized by the individual

§164.502

To Individuals

- Besides making required disclosures, Covered Entities may also disclose PHI to their patients or enrollees. For example:
  - Health plans may contact their enrollees.
  - Providers may contact or speak with their patients.
- Covered Entities must treat a personal representative -- person who has authority to make decision related to health care -- as an individual

Treatment, Payment, Health Care Operations (TPO)

- What is "treatment?"
- What is "payment?"
- What are "health care operations?"
- Using and disclosing for TPO §*164.506*
- Using and disclosing for TPO of other Covered Entities

§164.502

Opportunity to Agree or Object

- To use PHI in facility directories (name, location, general condition, religious affiliation to clergy)
- To disclose PHI to persons involved in care or payment for care and for notification purposes. For example:
  - Friends may pick up prescriptions.
  - Hospitals may notify family members of a patient's condition.
  - Covered entities may notify disaster relief agencies.

§164.510

Public Priorities

- Covered Entities may use or disclose PHI without authorization only if the use or disclosure comes within one of the listed exceptions and follows its conditions. Some examples:
  - As required by law
  - For public health activities
  - About victims of abuse, neglect, or domestic violence
  - For judicial and administrative proceedings
  - For specialized government functions

§164.512

Public Priorities, continued

- For health oversight activities
- For law enforcement purposes
- About decedents, to coroners, medical examiners, funeral directors
- For cadaveric organ, eye or tissue donations
- For research purposes
- For workers' compensation
- To avert a serious threat to health or safety

Incidental Uses and Disclosures

- The Privacy Rule permits uses and disclosures incidental to an otherwise permitted use or disclosure, provided minimum necessary and safeguard standards (discussed following) are met.
  - Examples: talking to a patient in a semi-private room; talking to other providers if passers-by are present; waiting-room sign-in sheets; patient charts at bedside.
- Allows for common practices if reasonably performed

§164.502

Minimum Necessary Standard

- Covered entities must make reasonable efforts to use, disclose, or request the minimum necessary ("MN") PHI based on purpose.
- Exceptions to the MN standard: e.g., disclosure of PHI for the purpose of treatment
- Covered entities must identify classes of workforce members who need access to PHI to do their jobs.
- Covered entities must develop criteria to limit disclosures of and requests for PHI to the MN.

§164.502

Case Example #1

- An employee and patient of an IHS facility left work for a doctor's appointment. The employee's supervisor wanted to verify that the employee was actually at a doctor's appointment, so he accessed the facility's scheduling system and confirmed that the employee did in fact have an appointment that day.
- The facility provided OCR the following documentation:
  - Confidentiality Agreements signed by all employees
  - Indian Health Service, Office of Information Technology, Division of Information Security, "General User Security Handbook"
  - System Access forms

Case Example #1 (cont'd)

- The employee's supervisor also called the doctor to confirm that the patient/employee had checked in for her appointment. The doctor confirmed that the employee had come in. During the investigation, the facility reported to OCR that the doctor did not disclose any of the patient/employee's PHI to the supervisor. The situation was resolved by the following:
  - OCR provided technical assistance regarding the definition of PHI
  - Facility issued a memo to all of its providers advising them that they may not release to an employer information about appointments and/or services provided to their employees without authorization
  - Facility provided training on the Privacy Rule to all workforce members
  - With OCR's technical assistance, the facility drafted a sanctions policy to apply to workforce members who violate the Privacy Rule

Authorizations

- Covered Entities *must* obtain an individual's authorization before using or disclosing PHI for purposes other than:
  - TPO;
  - Where the opportunity to agree or object is required;
  - Specified public priorities.
- Authorizations *must* be obtained for marketing (with limited exceptions).

§164.508

Administrative Requirements

- Covered Entities must:
  - Designate a Privacy Officer;
  - Designate a contact person or office to receive complaints and provide further information;
  - Provide privacy training to all workforce members;
  - Develop and apply sanction policy for workforce members who fail to comply;
  - Implement policies and procedures designed to comply with standards.

Administrative Requirements (cont.)

- Covered Entities must:
  - Implement administrative, technical and physical safeguards to protect privacy of PHI;
  - Mitigate any harmful effect of a violation known to the covered entity to the extent practicable;
  - Provide an internal complaint process for individuals;
  - Refrain from intimidating and retaliatory acts;
  - Not require individuals to waive their rights.

§164.530

Case Example #2

- Complainant worked in an IHS hospital where PHI was being faxed to fax machines that were located in unsecured areas of the hospital that were easily accessible to unauthorized individuals, and incoming faxes would be placed on an open, accessible table.
- After OCR provided technical assistance, the hospital took the following corrective actions:
  - Relocated the fax machine to a more secure area
  - Created an incoming fax holding bin (faxes placed face down)
  - Limited faxing PHI to only medical emergency situations
  - Limited the amount of information that can be included on a fax cover sheet

Individual Rights

- Notice of Privacy Practices
- Access: inspect and copy
- Amendment
- Accounting
- Alternative communications
- Request restriction
- Complaints to Covered Entity and Secretary

Notice

- Individual has the right to written notice of the uses and disclosures of PHI that may be made by CE, CE's legal duties with regard to PHI, and individual rights.
- Required elements in Privacy Rule
- In most cases, Covered Entity must post and provide a copy to the individual on first contact with providers and upon enrollment with health plan and upon request.
- Covered provider must document "good faith effort" to obtain acknowledgement.

§164.520

Access

- Individual has a right to inspect and obtain a copy of PHI about the individual in a designated record set ("DRS") for as long as the DRS is maintained.
- CE must act on the request within 30 days.
- CE must provide access in the form or format requested
- Reasonable fees are allowed for copying and postage only (no retrieval fees allowed).

§164.524

Case Example #3

- Complainant, a tribal member who worked for the tribe, requested a copy of her medical records from an IHS clinic. The clinic, instead of providing Complainant her records, sent the records to the Tribal Administrator, who, at the time, served as the Tribal Health Director. The facility had no policy designating appropriate access of PHI by clinic staff.
- OCR worked with the facility to achieve the following corrective action:

  - With technical assistance from OCR, the clinic created a policy and procedure regarding an individual's right to access his or her PHI
  - The clinic provided Complainant a copy of her records
  - With OCR's technical assistance, the clinic created a policy identifying the classes of persons in the workforce who needed access to PHI to carry out their duties

Amendment

- Amendment:

  An individual has the right to request that a CE amend PHI about the individual in a DRS as long as the DRS is maintained.

  §164.526

Accounting

- Accounting:

  An individual has the right to receive an accounting of disclosures of PHI made by a CE in the six years or less prior to the request.

  §164.528

Alternative Communication

- Alternative Communication

  A covered health care provider must permit the individual to request and must accommodate reasonable requests to receive communications of PHI by alternative means and at alternative locations. The requirement applies to health plans if the individual clearly states that the disclosure could endanger the individual.

  §164.522(b)

Request Restrictions

- Request Restrictions

  CE must permit the individual to request that the CE restrict uses and disclosures of PHI for TPO. CE not required to agree to the request.

  §164.522(a)

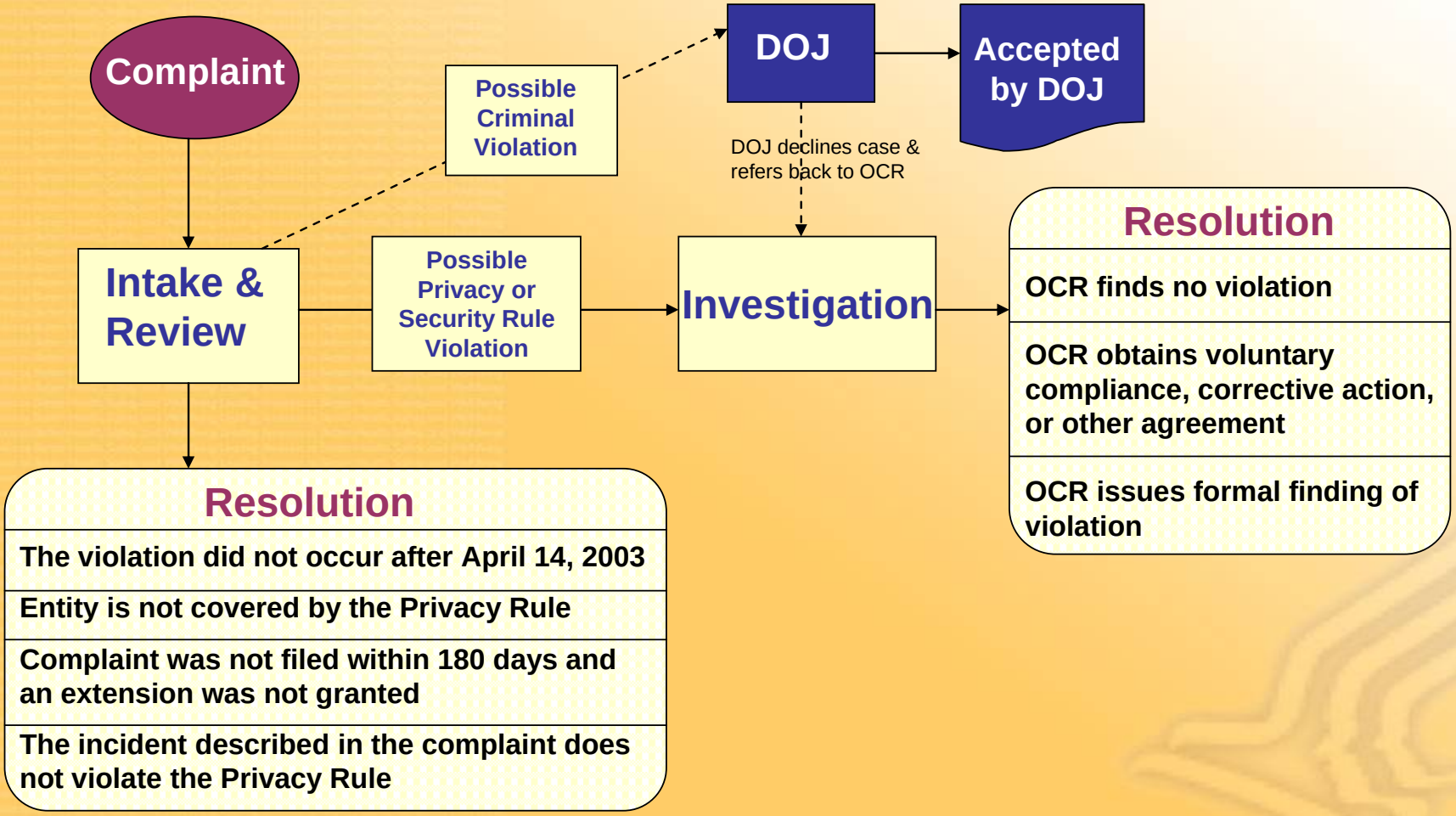
Case Example #4

- Complainant alleged that employees working for a Tribal Health Systems Department accessed PHI from an IHS facility computer
- OCR encouraged the Nation and IHS to develop policies and procedures regarding access to computer systems and safeguarding PHI
- The Nation and IHS met and produced a Memorandum of Understanding (MOU) that was signed by the Tribal Chairman, the IHS Area Director, and the IHS Contracting Officer

Complaint Investigations

- Every complaint received by OCR is reviewed and allegations analyzed.
- An investigation is launched when warranted by the facts and circumstances presented by the complaint.
- OCR investigations have resulted in changes in privacy practices and other corrective actions in over 9,854 cases since April 2003.
- Corrective action obtained by HHS from covered entities has resulted in systemic change that benefits all individuals they serve.

HIPAA Privacy and Security Rule Complaint Process



Civil Money Penalty Amounts

	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**

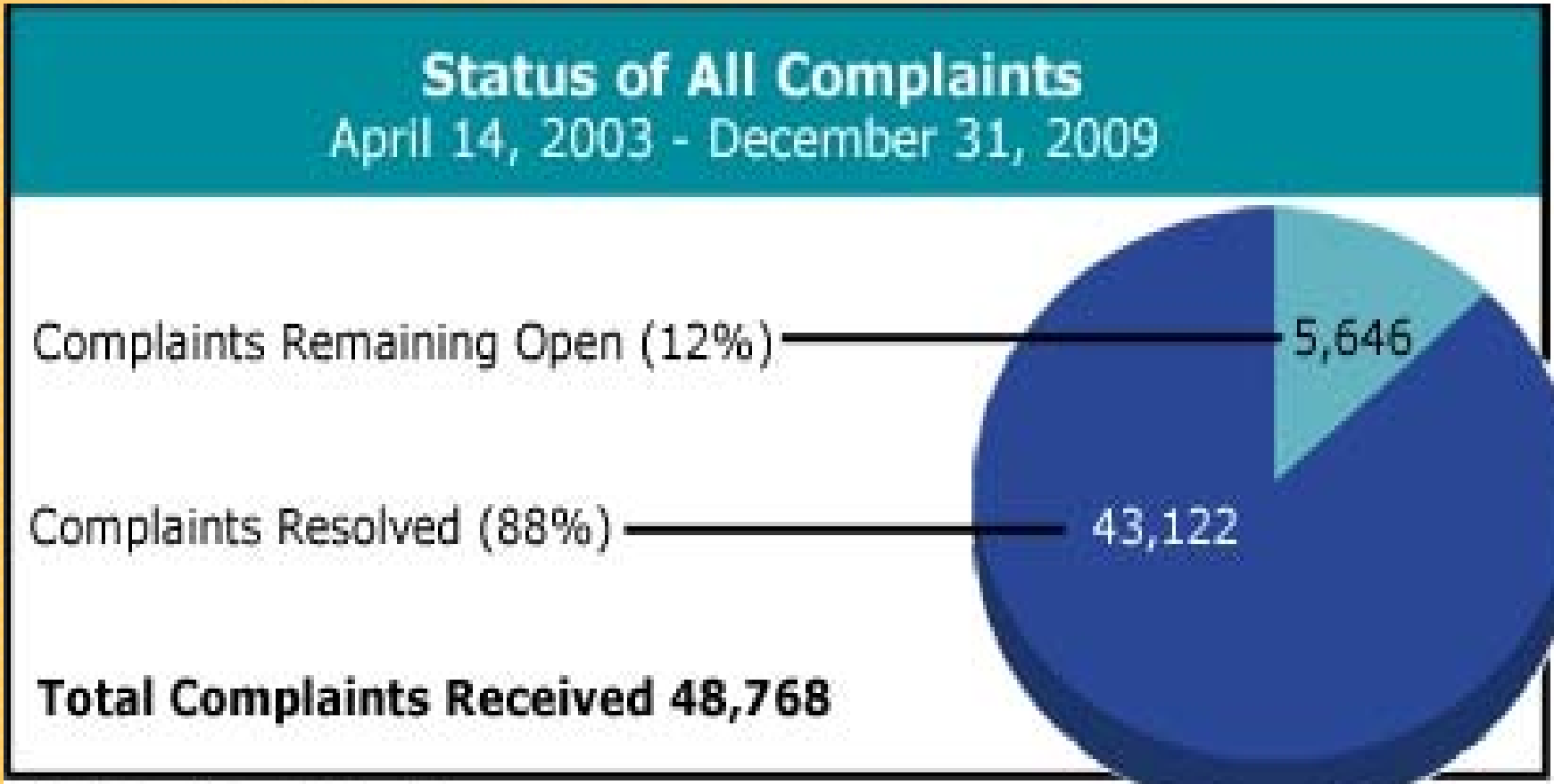
- OCR may reduce a penalty if the failure to comply was due to reasonable cause and not willful neglect, and the penalty would be excessive relative to the noncompliance.

Affirmative Defenses

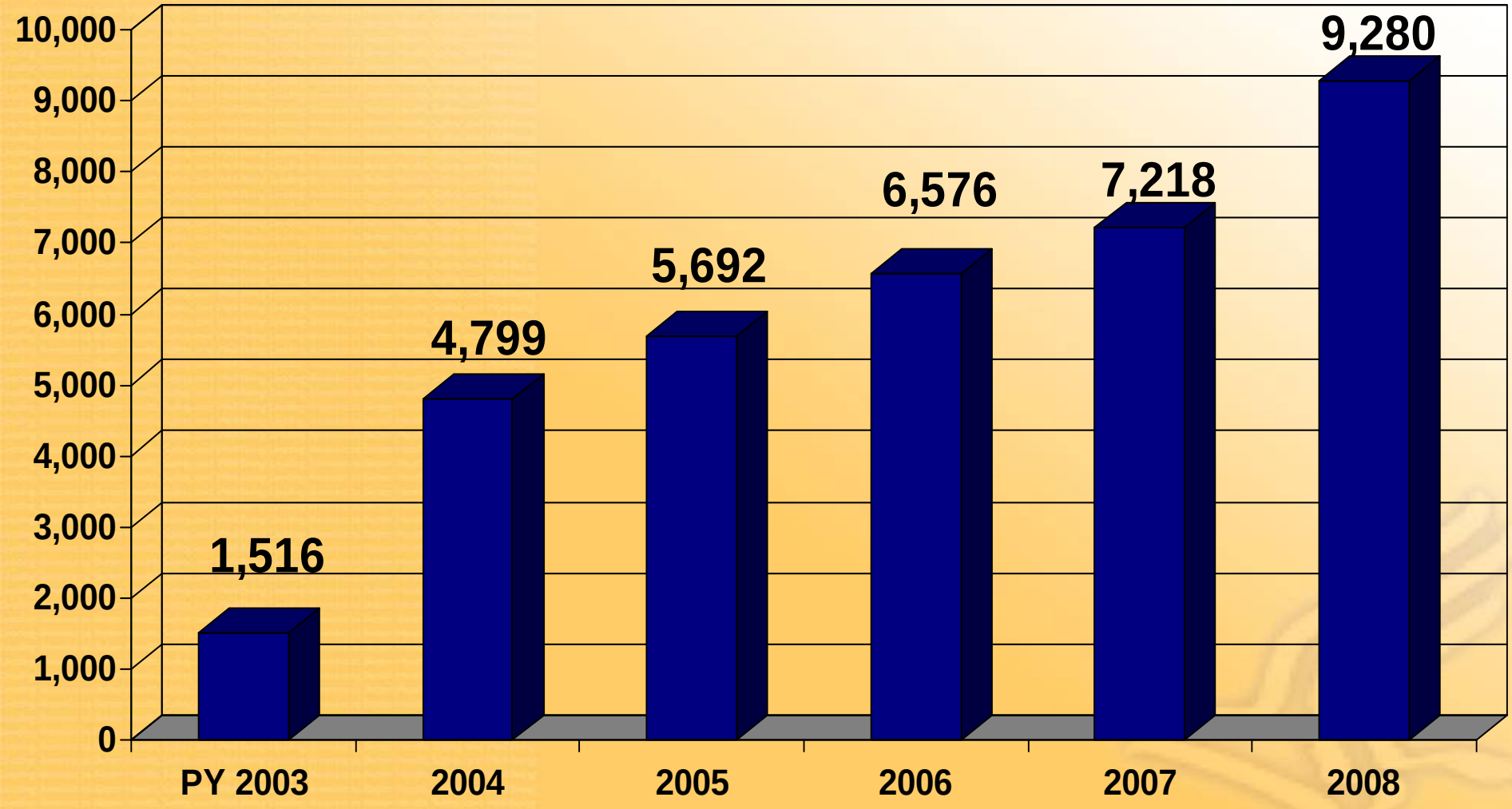
- **Violations Occurring Before the HITECH Act** (before February 18, 2009):
  - Disclosure is punishable criminally under § 1177;
  - CE did not know and reasonably would not have known that violation occurred; or
  - Reasonable cause and not willful neglect, and corrected during 30-day time period.

- **Violations Occurring After the HITECH Act** (on or after February 18, 2009):
  - Disclosure is punishable criminally under § 1177 (until February 17, 2011);
  - Disclosure is punished criminally under § 1177 (on or after February 17, 2011); or
  - Not due to willful neglect and corrected during 30-day time period.

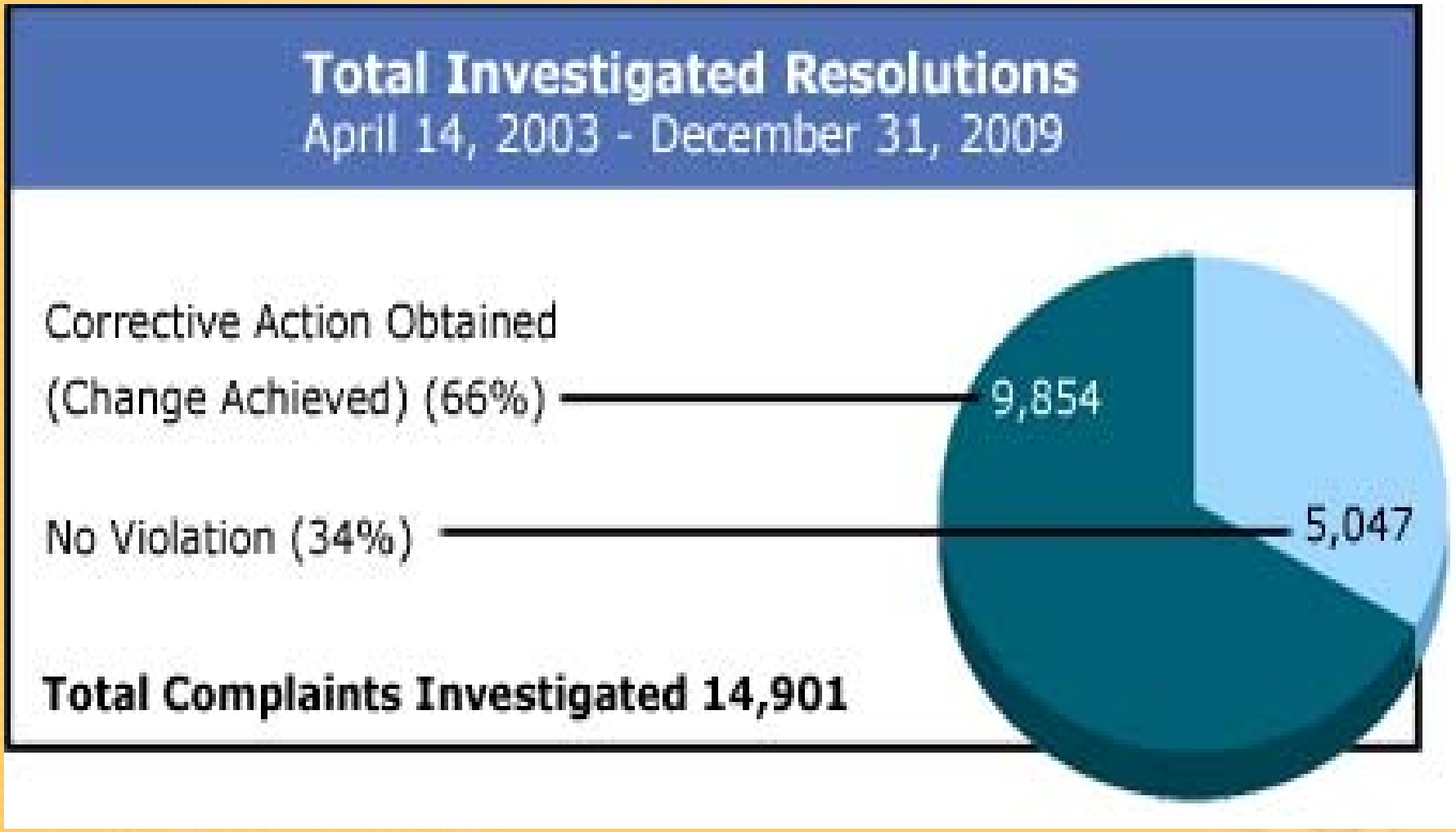
Pie Chart: All Complaints



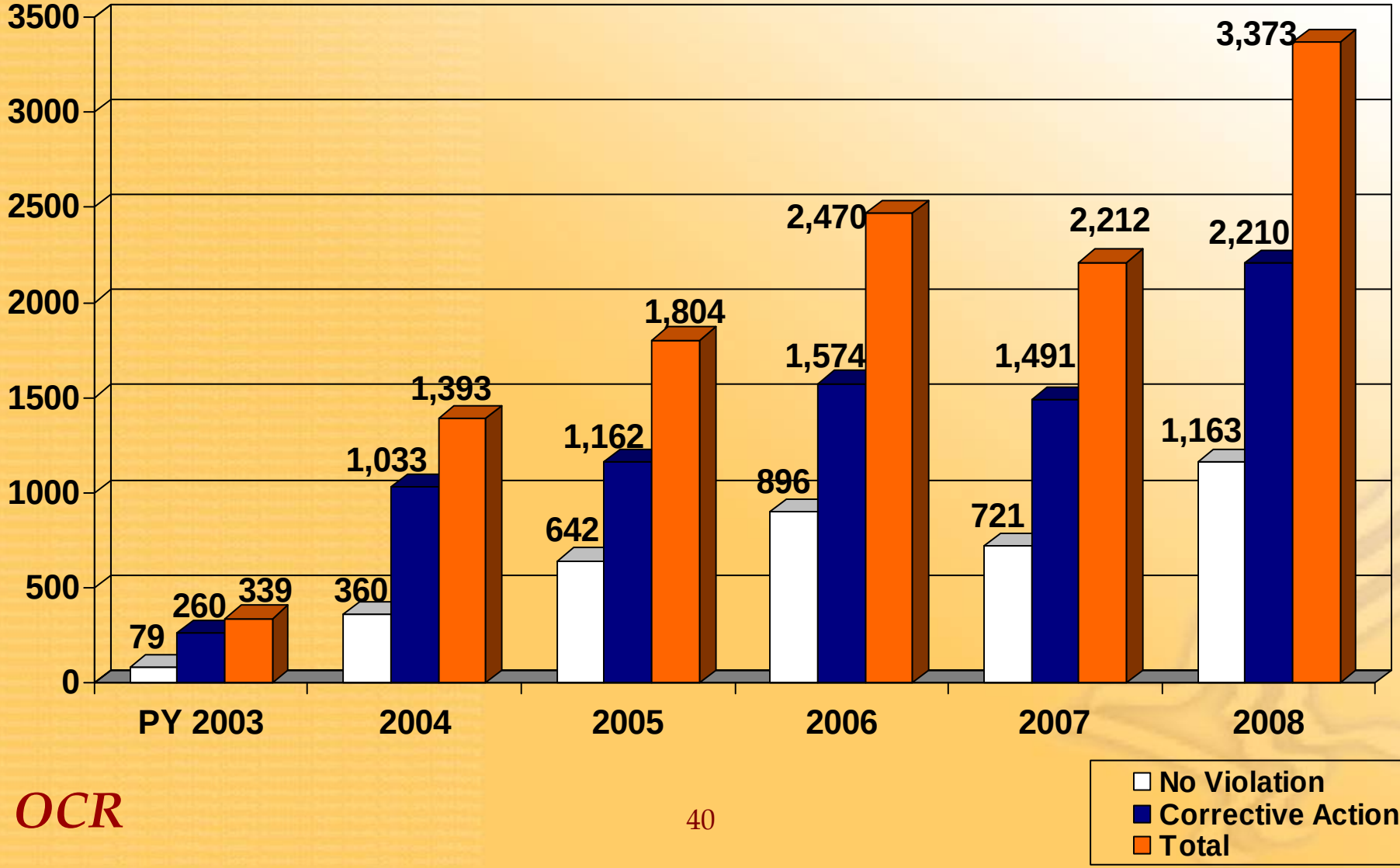
Total Resolutions by Calendar Year



Pie Chart: Total Investigated



Investigated Resolutions



Complaints against IHS facilities

- Number of complaints investigated during the 2008 and 2009 calendar years
- Number of currently open complaints
- Most common issues raised

Complaints against tribally-run facilities

- Number of complaints investigated during the 2008 and 2009 calendar years
- Number of currently open complaints
- Most common issues raised

Issues in Enforcement Actions

(April 14, 2003 to December 31, 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 protected health information
- Failure to have the individual's valid authorization for a disclosure that requires one

Covered Entities in Enforcement Actions
(April 14, 2003 to December 31, 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

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.

Tips for CE Privacy/Security Officers During an OCR Investigation

- When notification letter is received, contact investigator named in letter. Establish effective communication with investigator. Contact investigator for assistance with questions, such as, “How does this work…?”
- Respond within stated time frames. If CE cannot make the due date, let investigator know. Request a reasonable extension of time – enough so CE can accomplish the requested task. Avoid multiple requests for time extensions. Return telephone calls from the OCR investigator promptly.

Investigation Tips (cont'd)

- If CE is aware of a Privacy/Security Rule incident even before receiving notification letter, start gathering relevant materials and facts. Formulate corrective action plan (CAP) and execute it. An executed CAP will then be ready to deliver to the investigator when notification letter is received.
- Be specific in your responses to requests for data and information. For example, if training was provided, provide all the facts – when, who was trained (sign-in sheet), topics covered; if a policy has been revised, send a copy of the old policy and the new policy. Do not send entire privacy/security policies and procedures manual unless specifically requested.

Investigation Tips (cont'd)

- Understand that investigations take place over an extended period of time. OCR investigator will work hard to be timely, but some investigations take longer than others.
- Be cooperative with the OCR investigator. Facts need to be confirmed by OCR. If OCR requests to interview an employee or requests contact information for former employees, provide this information in a timely manner. If you cannot, explain why.
- Ask for technical assistance if you do not understand what is expected by a particular requirement of the Privacy or Security Rules.

Investigation Tips (cont'd)

- Be forthcoming and acknowledge errors if they occurred. Remember, the goal is resolution through voluntary compliance and completed corrective action.
- Respond. Ignoring the investigation will exacerbate the matter.

Topics

- Privacy and Security Rule Enforcement
- Other Challenges
  - Genetic Non-Discrimination
  - Patient Safety Act
  - Health Information Technology
  - Emergency Preparedness
  - Getting Out the Message
  - Other Program Challenges
- Breach

Our Mutual Goal

Ensuring the privacy and security of each individual's health information in accordance with the standards and requirements of the HIPAA Privacy and Security Rules

OCR Web Site

- http://www.hhs.gov/ocr/hipaa/
- The full text of the Privacy and Security Rules
- HIPAA Privacy Rule summary
- Covered entity "decision tool" to assist individuals and entities in making these determinations
- Over 200 frequently asked questions
- Fact sheets
- Information about the OCR enforcement program