U.S. Department of Health & Human Services

Office for Civil Rights

Indian Health Service 14th National Partnerships Conference Denver, Colorado

August 13, 2013

The Office for Civil Rights

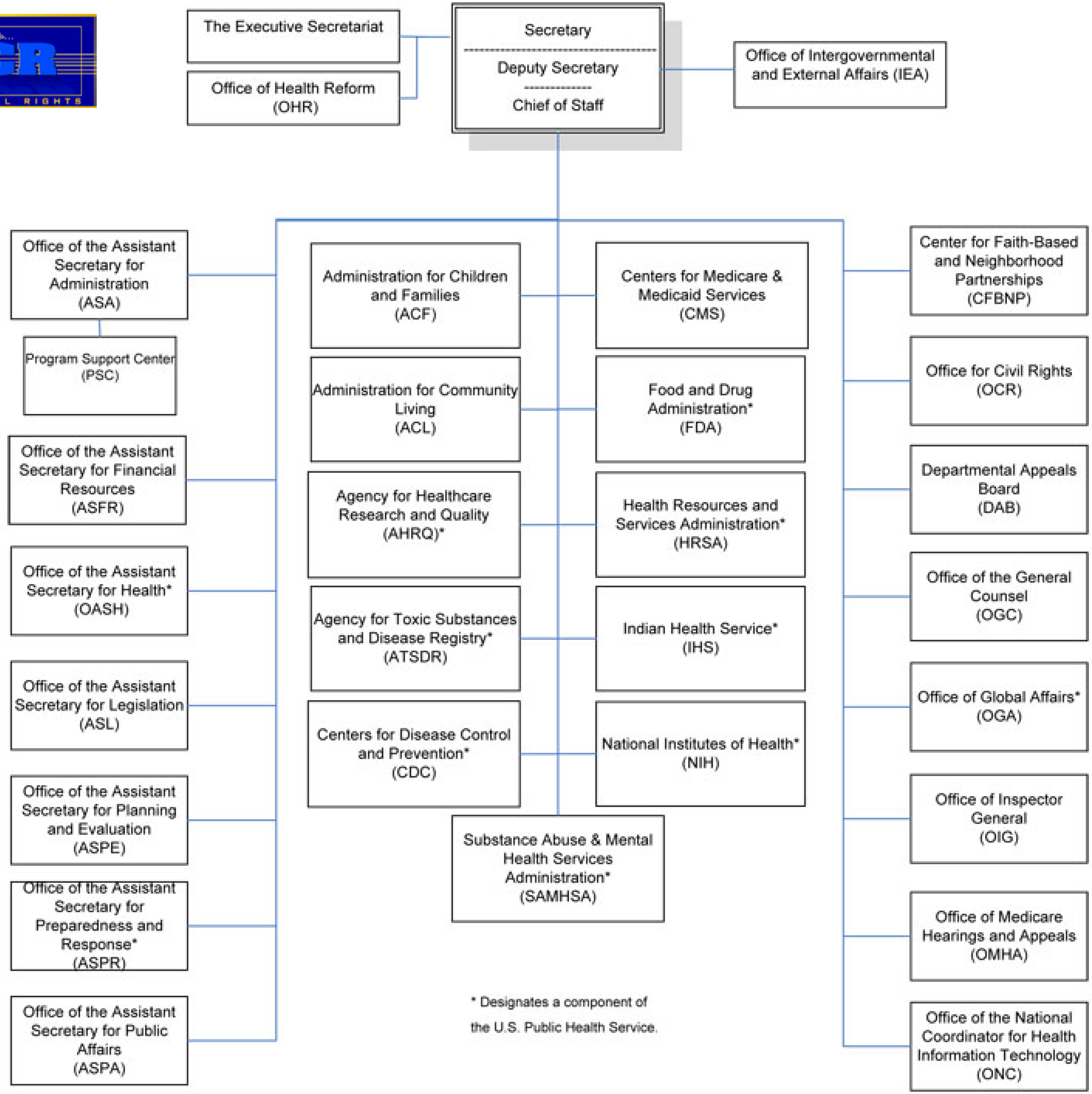
- OCR's director is Leon Rodriguez, J.D., former Chief of Staff, U.S. Department of Justice, Civil Rights Division.

- OCR is a component of the Office of the Secretary at HHS.

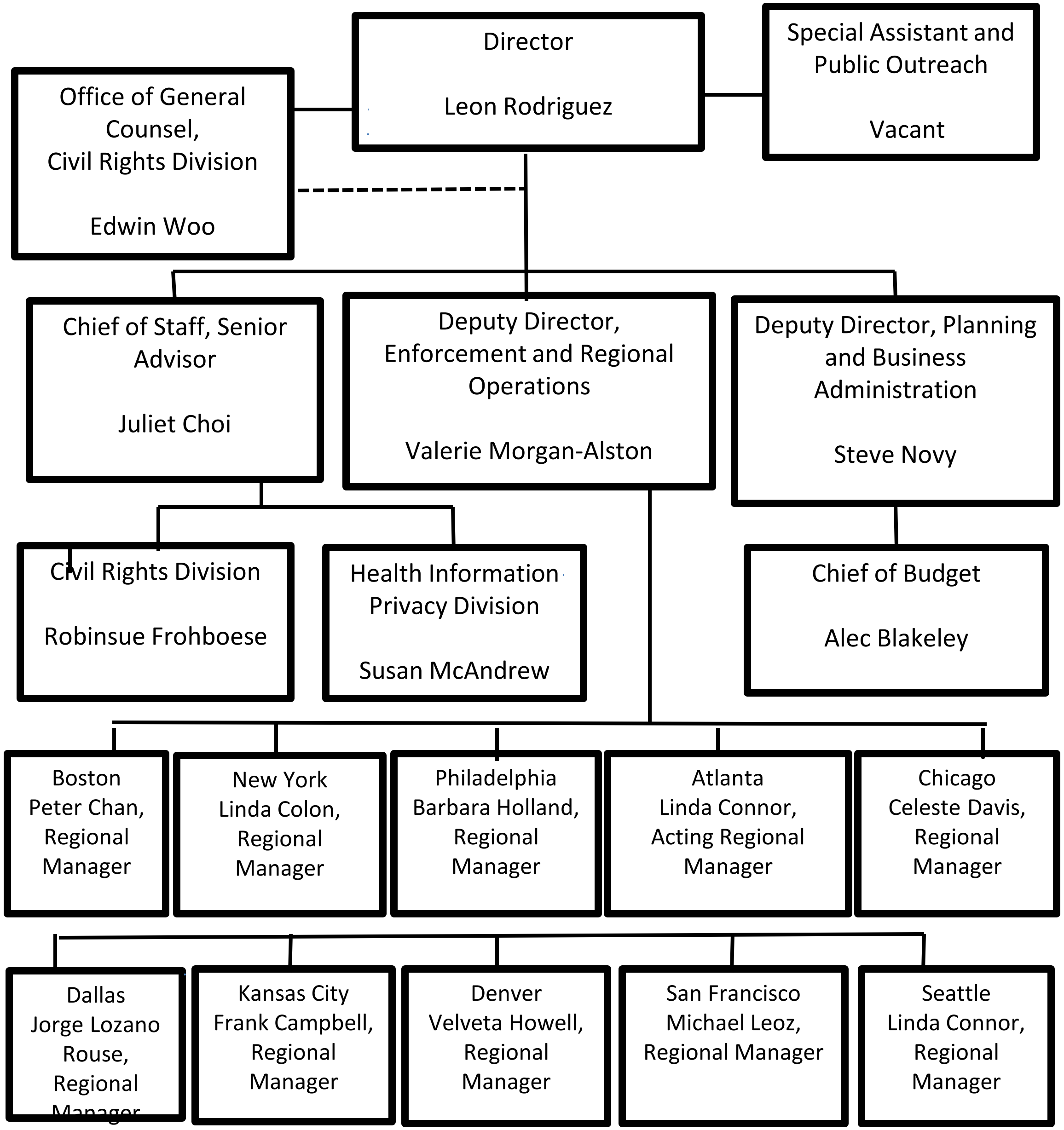
- OCR has approximately 230 staff in 10 regional offices and at its D.C.-based headquarters.

U.S. Department of Health & Human Services (DHHS)

- **Office of the Secretary**
  - Administration on Community Living, formerly the Administration on Aging
    - Office for Civil Rights
    - Office of the General Counsel
- Administration for Children and Families
- Agency for Healthcare Research & Quality
- Agency for Toxic Substances & Disease Registry
- Centers for Disease Control
- Food & Drug Administration
- Centers for Medicare & Medicaid Services
- Health Resources & Services Administration
- Indian Health Service
- National Institutes of Health
- Program Support Center
- Substance Abuse and Mental Health Services Administration


The Executive Secretariat
Office of Health Reform (OHR)
Secretary
Deputy Secretary
Chief of Staff
Office of Intergovernmental and External Affairs (IEA)
Office of the Assistant Secretary for Administration (ASA)
Program Support Center (PSC)
Office of the Assistant Secretary for Financial Resources (ASFR)
Office of the Assistant Secretary for Health* (OASH)
Office of the Assistant Secretary for Legislation (ASL)
Office of the Assistant Secretary for Planning and Evaluation (ASPE)
Office of the Assistant Secretary for Preparedness and Response* (ASPR)
Office of the Assistant Secretary for Public Affairs (ASPA)
Administration for Children and Families (ACF)
Administration for Community Living (ACL)
Agency for Healthcare Research and Quality (AHRQ)*
Agency for Toxic Substances and Disease Registry* (ATSDR)
Centers for Disease Control and Prevention* (CDC)
Centers for Medicare & Medicaid Services (CMS)
Food and Drug Administration* (FDA)
Health Resources and Services Administration* (HRSA)
Indian Health Service* (IHS)
National Institutes of Health* (NIH)
Substance Abuse & Mental Health Services Administration* (SAMHSA)
Center for Faith-Based and Neighborhood Partnerships (CFBNP)
Office for Civil Rights (OCR)
Departmental Appeals Board (DAB)
Office of the General Counsel (OGC)
Office of Global Affairs* (OGA)
Office of Inspector General (OIG)
Office of Medicare Hearings and Appeals (OMHA)
Office of the National Coordinator for Health Information Technology (ONC)
* Designates a component of the U.S. Public Health Service.

Department of Health and Human Services
Office for Civil Rights



What is the Office for Civil Rights (OCR)?

- OCR is a critical DHHS enforcement agency.
  - OCR enforces the HIPAA Privacy and Security Rules and HITECH.
  - OCR also enforces numerous traditional civil rights laws.
  - Laws include the nondiscrimination provisions of GINA and Section 1557 of the Affordable Care Act.

OCR's Missions

- To ensure people have equal access to and an opportunity to participate in and receive services from DHHS-funded and other covered programs without facing unlawful discrimination.

- To promote confidentiality in and access to protected health information.

- To promote the security of health information.

Jurisdiction and Authority

- **Program Jurisdiction**

  - OCR has jurisdiction over all providers of health and human services or benefits, such as:

* State agencies
* Hospitals
* Nursing homes
* Public health clinics
* Child service agencies
* Rural health agencies
* Adult day activity programs
* Medical schools and other health care programs
* Welfare programs
* Substance abuse treatment centers
* Medicaid Health Mgt. Organizations (HMOs)
* Outpatient rehabilitation clinics
* Home health agencies and hospices
* Area agencies on aging

Jurisdiction and Authority

- **Financial Jurisdiction**

  - Many agencies and programs must receive federal financial assistance. Some forms of federal financial assistance are:

    * Medicare, Part A
    * Medicaid
    * Temporary Assistance To Needy Families (TANF) Block Grants
    * Hill-Burton Funded Healthcare Facilities
    * Research grants from the National Institutes of Health
    * Title IV-E (children services – adoptive and foster care placements)
    * Ryan White Care Act funds (AIDS, HIV)

    * ***Exception***:
      --Public Entities subject to Title II of the Americans with Disabilities Act (ADA) of 1990 do not need to be recipients of federal financial assistance
      --HIPAA Privacy and Security Rules

OCR's Traditional Civil Rights Law Enforcement

- Regulations prohibiting race, color, national origin, age, disability, religion, and gender discrimination by recipients of Federal financial assistance (FFA) from DHHS.

- Regulation prohibiting disability discrimination by public entities (Title II of the Americans with Disabilities Act).

- Regulation prohibiting discrimination based on race, disability, age, national origin, sex (gender orientation), religion in DHHS funded and conducted programs (Section 1557, effective 3/23/2010). (Nondiscrimination Provisions of the Affordable Care Act).

Strategies to Achieve Civil Rights Compliance

- OCR uses the following strategies to facilitate civil rights compliance:

  - Complaint Process
  - Compliance Reviews
  - Public Policy
  - Technical Assistance

What is the Office for Civil Rights (OCR)?

- OCR is a critical DHHS enforcement agency.
  - OCR enforces the HIPAA Privacy and Security Rules.
  - OCR also enforces approximately 19 traditional civil rights laws.
  - Laws include the nondiscrimination provisions of GINA and Section 1557 of the Affordable Care Act.

- **Technical Assistance (TA)**

- OCR uses TA to resolve a complaint and compliance reviews when an FFA recipient is willing and able to voluntarily comply.

- OCR also uses TA to monitor settlement agreements.

- OCR offers outreach and shares information to FFA recipients, public entities, community organizations and other interested parties.

What Does OCR Do?

- Complaint Process –

  - Complaints must be filed within 180 days from the date of date of the alleged discriminatory act, unless:

    - the complainant demonstrates ongoing, systemic discrimination. or
    - good cause is shown for the delay in filing.

What Does OCR Do?

- Complaint Process - Who can file a complaint?

  - Individuals who believe they have been discriminated against by a covered entity (e.g., health care or human service provider), in the provisions of services based on their race, color, national origin, disability status, age, or, in certain limited circumstances, their sex or religion.
  - An organization or person, filing on behalf of an individual/ individuals, alleging either individual or systemic violations.

What Does OCR Do?

- Complaint Process - What happens next?
  - OCR determines jurisdiction.
  - One or more OCR Equal Opportunity Specialists investigate the complaint.
  - A decision is released in a Letter of Findings (LOF).
  - Corrective actions will be required to ensure compliance where issues are substantiated.
  - Settlement agreement, incorporating corrective actions may be signed by covered entities and OCR.
  - OCR may commence enforcement proceedings if a covered entity will not comply voluntarily.

What Does OCR Do?

- If OCR has reason to believe a covered entity is not complying with federal civil rights or HIPAA laws, it may initiate an investigation itself through a compliance review.

- Compliance reviews may involve:

  - Data requests
  - Interviews
  - Observation
  - Research
  - Technical Assistance

OCR Priority Areas

- **Current Policy Priority Areas**

  -Health Disparities Initiative: Partners with stakeholders to identify and address racial disparities in health care.

  -Olmstead Community Living Initiative: Collaborates with states and other stakeholders in development of comprehensive plans pursuant to *Olmstead v. L.C.*, *et al*., U.S. Supreme Court, June 1999).

  -Critical Access Hospitals Initiative: Promotes access to designated facilities' services for persons with limited English proficiency (LEP).

OCR Priority Areas (con't.)

-LEP Initiative: Works with human services and health agencies and providers, including managed care organizations, to ensure equal access for limited-English proficient persons.

Language Access Plan: Enhances limited English proficient (LEP) persons' access to HHS-funded programs.

-Hospital Effective Communications Initiative: Collaborates with state hospital associations to promote access to healthcare facilities for LEP and deaf and hard-of-hearing populations.

-Medical Education Initiative: Partners with medical schools to train future doctors on Title VI to promote access to facilities for LEP and other vulnerable populations.

Karel Hadacek, J.D.

Equal Opportunity Specialist

U.S. Dept. of Health & Human Services

Office for Civil Rights

Who must follow the Privacy Rule?

- Three categories of covered entities:
  - Health plans
  - Health care clearinghouses
  - Health care providers who transmit health information electronically in connection with certain administrative and financial transactions

HIPAA Regulation - Coverage

- “Covered entities” - health care providers who electronically transmit health information in connection with a standard transaction; health plans; health care clearinghouses
- Hybrid entities (e.g., HHS)
- Business associates (contract usually required)

Business Associates

Agents, contractors, and others hired to do the work of, or to work for, the covered entity, and such work requires the use or disclosure of PHI.

Business Associates

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.

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.

Scope: What is Covered?

- Not PHI:
  - De-identified information
  - Employment records
  - FERPA records

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.

Permissive Uses and Disclosures

Without authorization, subject to conditions:

- For treatment, payment, and health care operations (TPO)

Incidental Use and Disclosures

- The Privacy Rule permits uses and disclosures incidental to an otherwise permitted use or disclosure, provided minimum necessary and reasonable safeguard standards 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

Public Priorities

- Covered entities may use or disclose PHI under these provisions if required conditions are met:
  – As required by law
  – For public health activities
  – About victims of abuse, neglect or domestic violence
  – For health oversight activities
  – For judicial and administrative proceedings

Public Priorities

- For law enforcement purposes
- To coroners, medical examiners, funeral directors
- For cadaveric organ, eye, or tissue donation purposes
- For research purposes
- To avert a serious threat to health & safety
- For specialized government functions
- For workers' compensation

Minimum Necessary Standard

- Covered entities must make reasonable efforts to use, disclose, or request the minimum necessary PHI based on purpose.

- Exceptions to the minimum necessary standard: e.g., disclosure of PHI for the purpose of treatment

Individual Rights

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

Individual Rights
Notice of Privacy Practices

- 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. (*Notice of Privacy Practices)*

- Required elements in Privacy Rule

Individual Rights

- 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.

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.

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;

Administrative Requirements

- Implement policies and procedures designed to comply with standards.
  - 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;

Administrative Requirements

– Provide an internal complaint process for individuals;

– Refrain from intimidating and retaliatory acts;

– Not require individuals to waive their rights.

Security Rule

Workforce Security

- Authorization and/or supervision
- Workforce clearance
- Termination procedures
- Information access management
- Security awareness and training

Security Rule

Physical Security

- Facility access controls
- Workstation use
- Workstation security
- Device and Media Controls

Security Rule

Technical Security

- Access Control
  - Unique User Identification
  - Emergency Access procedure
  - Automatic Log-off
  - Encryption/Decryption

HITECH and HIPAA

- 2009 HITECH Act
  - Standards for electronic records and data sharing in clinical setting, for quality reporting, and other population health purposes
  - Subpart D for privacy protections and security for patient identifiable information

Breach Notification

- Covered entities must notify each affected individual of breach of “unsecured protected health information.”

- Business associate must notify covered entity of breach

Breach Notification

- Notice to media if more than 500 people affected.
- Notifications to be provided without unreasonable delay (but no later than within 60 days) of discovery of breach.
- Notice to Secretary of breach and posting on HHS Website.

Compliance and Enforcement

- Any person or organization can file complaints with OCR (generally within 180 days)
- OCR may investigate complaints and may conduct compliance reviews
- Covered entity must provide OCR with access to records; subpoena authority
- OCR shall attempt to resolve noncompliance by informal means

Omnibus Final Rule – Important Dates

- Public Display at Federal Register – January 17, 2013
- Published in Federal Register – January 25, 2013
- Effective Date – March 26, 2013
- Compliance Date – September 23, 2013
- Conform BA contracts – September 22, 2014

Omnibus– What's New for Consumers

- Right to Electronic Copy of Electronic Health Record
  - Right to direct copy to designated 3d party
- Prohibition on Sale of PHI without Authorization
- Marketing Communications Paid for by 3d Party Require Authorization
  - Limited exceptions for refill reminders and current prescriptions
- Easy Way to Stop Fundraising Communications
- Right to Restrict Disclosures to Health Plans of Treatment/Services Paid for Out of Pocket

Omnibus– Electronic Access

- If individual requests e-copy of PHI maintained electronically in designated record set, covered entity must provide access in electronic form/format requested, if readily producible, otherwise in readable electronic form/format as agreed to by covered entity and individual
  - Must be able to produce some form of e-copy
  - Can provide hard copy if individual declines to accept any of the electronic formats of the covered entity

Omnibus– Electronic Access

- If requested, covered entity must transmit copy of PHI to individual's designee (not limited to electronic access)
  - Request must be in writing & signed
  - Must clearly identify designated person and where to send

Omnibus– Non-Statutory Provisions

- Student Immunization
  - Makes it easier for parents to permit providers to release student immunization records to schools
- Research
  - Allows researchers to use single authorization for more than one research purpose
  - Relaxes policy on authorizations for future research

Omnibus– Non-Statutory Provisions

- Notice of Privacy Practices
  - Updates required to Notices of Privacy Practices
  - Relaxes distribution requirements for Health Plans

- Decedent Information
  - Protections limited to 50 years after death
  - Eases access to friends and families

Omnibus– Notice of Privacy Practices

- Content must now include:
  - Statements regarding sale of PHI, marketing, and other purposes that require authorization
  - For covered entities engaging in fundraising, statement that individual can opt out of fundraising communications
  - For providers, statement that covered entity must agree to restrict disclosure to health plan if individual pays out of pocket in full for health care service
  - Statement about individual's right to receive breach notifications
  - For plans that underwrite, statement that genetic information may not be used for such purposes

Omnibus– Notice of Privacy Practices

- Health plans may distribute materially revised NPPs:
  - By posting on web site by effective date of change and including in next annual mailing to individuals; or
  - Mailing to individuals within 60 days of material revision

Omnibus– Business Associates

- BAs must comply with the technical, administrative, and physical safeguard requirements under the Security Rule; liable for Security Rule violations
- BA must comply with use or disclosure limitations expressed in its contract and those in the Privacy Rule; criminal and civil liabilities attach for violations
- BA definition expressly includes Health Information Organizations, E-prescribing Gateways, and PHR vendors that provide services to covered entities
- Subcontractors of a BA are now defined as a BA; clarifying that BA liability flows to all subcontractors

Omnibus– New for Breach

- Breach Notification Provisions
  - Replaces “harm to individual” with more objective measure of compromise to the data as threshold for breach notification
  - Other provisions of 2009 IFR adopted without major change

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.

Complaint Investigations

- Corrective action obtained by HHS from covered entities has resulted in systemic change that benefits all individuals they serve.

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 Rule

Indications of Noncompliance

45 CFR 160.312: If investigation or compliance review indicates noncompliance, HHS will attempt to reach resolution satisfactory to the Secretary by "informal means."

Indications of Noncompliance

- When OCR determines from its investigation of the allegations raised in a Privacy Rule complaint or through a compliance review that a covered entity may well have violated the Privacy Rule and/or the Security Rule, OCR has various means of enforcement at its command.

Methods of Enforcement

- If feasible, OCR usually seeks voluntary compliance. Voluntary compliance often involves the covered entity changing its policies and procedures, retaining personnel, and sanctioning the members of its workforce who violated the Privacy or Security Rules.

Methods of Enforcement

- If OCR determines that the conduct involved warrants some sort of penalty even if voluntary compliance is forthcoming, OCR may seek to have the covered entity enter into a Resolution Agreement and Corrective Action Plan as well as pay a "resolution amount." This method is often used when the problems identified by OCR are systemic.

Methods of Enforcement

- If OCR either determines that the conduct involved is so serious or if the covered entity is adamant in its refusal to cooperate in the investigation or resolution of the problem, OCR will assess a Civil Money Penalty (CMP).

Breach Notification Highlights

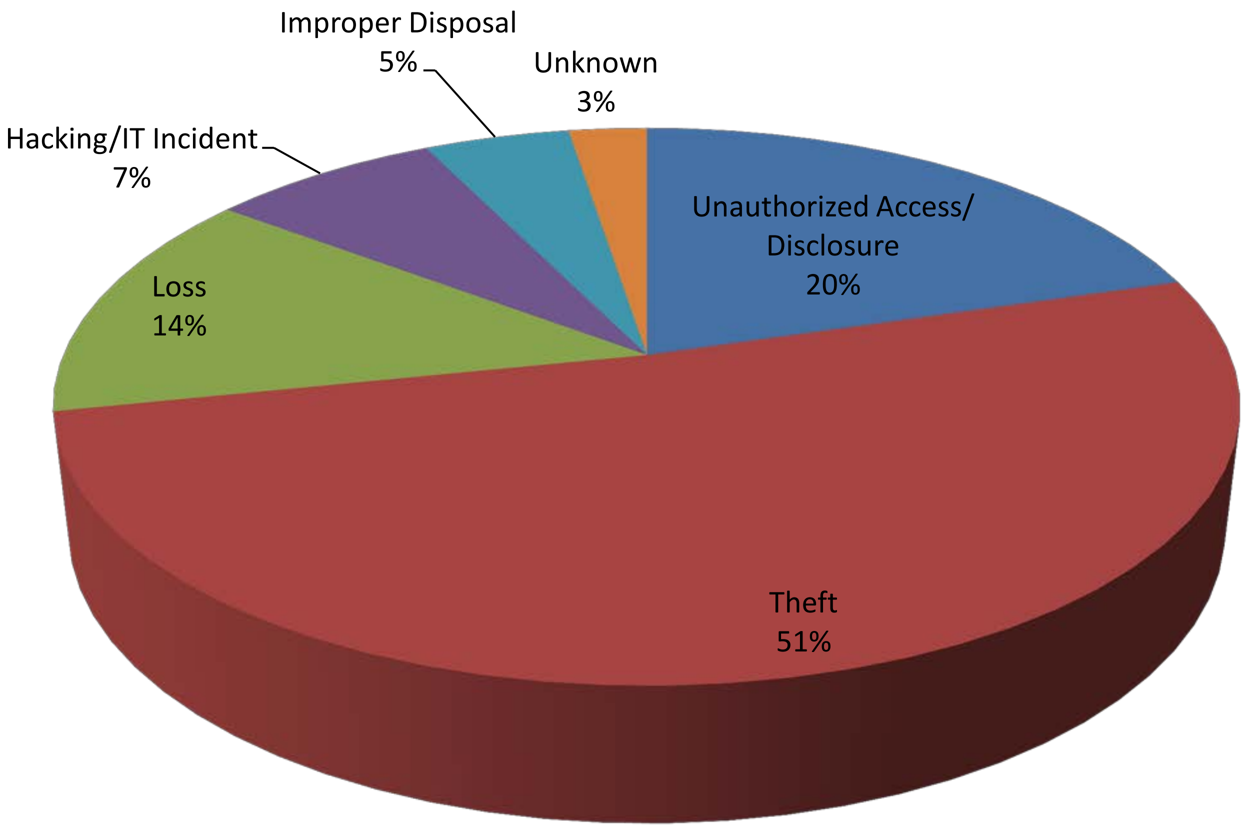
September 2009 through February 20, 2013

- 543 reports involving over 500 individuals
- Over 64,000 reports involving under 500 individuals
- Top types of large breaches
  - Theft
  - Unauthorized Access/Disclosure
  - Loss
- Top locations for large breaches
  - Laptops
  - Paper records
  - Desktop Computers
  - Portable Electronic Device

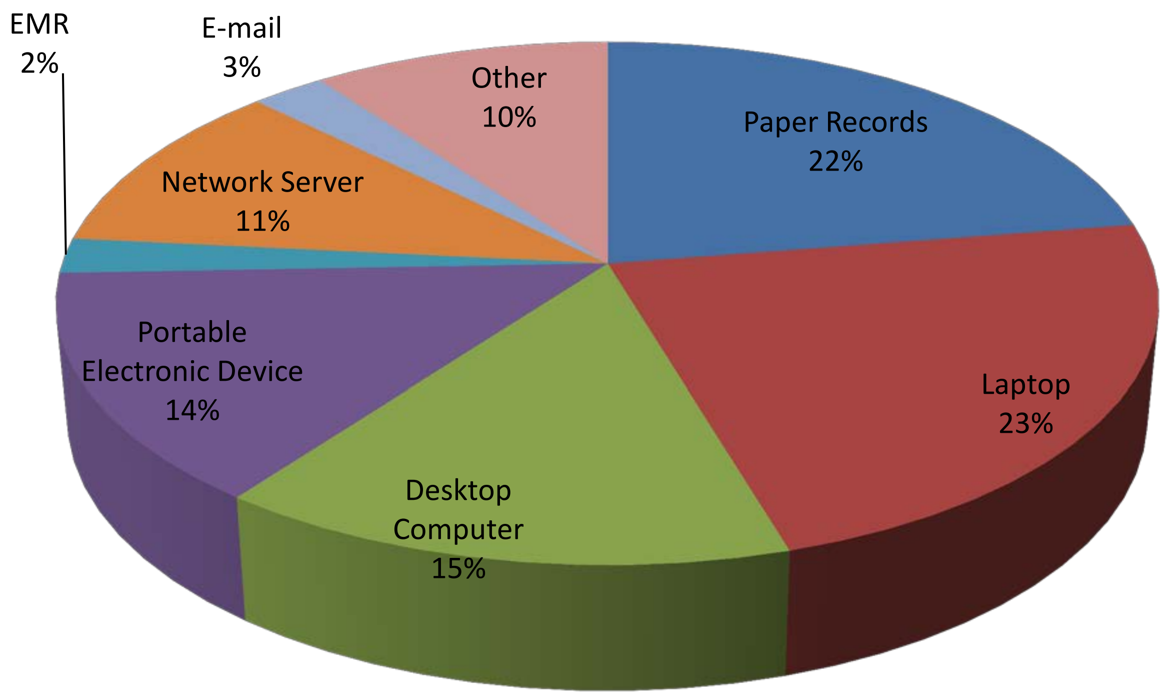
Spotlight on Largest Breaches of 2012

- Hacking network server – 780,000 affected
- Backup tapes stored at hospital cannot be found and are presumed lost– 315,000 affected
- Unencrypted emails sent to employee’s unsecured email address -- 228,435 affected
- Theft of laptop from employee’s vehicle– 116,506 affected
- Unauthorized access to e-PHI stored in database-- 105,646 affected
- Hacking database stored on network server – 70,000 affected

Breach Notification:
500+ Breaches by Type of Breach



Breach Notification: 500+ Breaches by Type of Location



OCR Web Site

www.hhs.gov/ocr

Privacy: www.hhs.gov/ocr/hipaa/

OCR Web Site

FAQs

http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html

Additional Information

- On HIPAA Privacy Rule protections and requirements: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

Additional Information

- On HIPAA Privacy Rule resolution agreements and other enforcement actions: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html

OCR Web Site

Karel Hadacek, J.D.

Equal Opportunity Specialist

U.S. Dept. of Health & Human Services

Office for Civil Rights

Karel.Hadacek@HHS.gov

303-844-7836

Contact Information

OCR, Region VIII

Regional Manager: Velveta Howell

Office for Civil Rights

U.S. Department of Health and Human Services

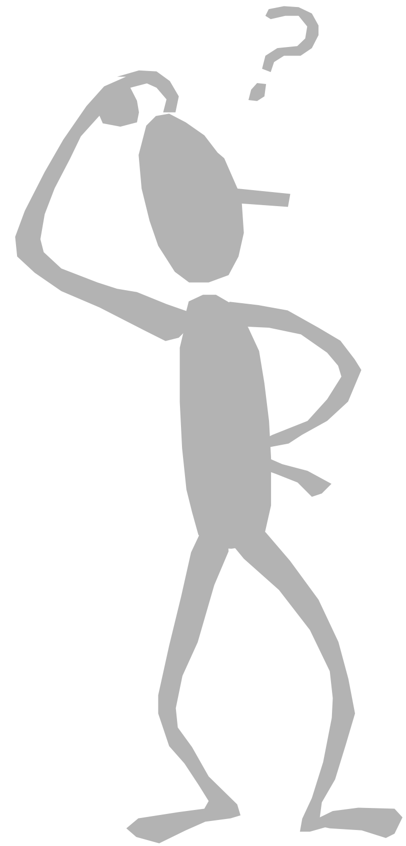
999 18th Street, South Terrace, Suite 417

Denver, CO 80202

E-mail: Velveta.Howell@hhs.gov

Voice: (303) 844-7915

TDD: (303) 844-3439



Contact Information

OCR Headquarters

U.S. Department of Health & Human Services

Office for Civil Rights, Room 509F

200 Independence Avenue, S.W.

Washington, D.C. 20201

Website: www.hhs.gov/ocr

Voice :(202) 619-0403

TDD: (800) 537-7697