Office for Civil Rights: An Overview of OCR and Our Legal Authorities

Michael Leoz, Regional Manager
Megan Yelorda, Equal Opportunity Specialist

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

An Introduction to OCR

What Is the Office for Civil Rights (OCR)?

- Part of the U.S. Department of Health and Human Services
- Enforces a number of civil rights laws as they relate to recipients of Federal financial assistance (FFA) from HHS, public entities, and programs & activities conducted by HHS
- Enforces the HIPAA Privacy, Security, and Breach Notification Rules
- Headquartered in D.C. with 8 regional offices (in 11 locations) across the U.S.

What Is the Office for Civil Rights (OCR)?

- New England (Boston)
- Eastern and Caribbean (New York)
- Mid-Atlantic (Philadelphia)
- Southeast (Atlanta)
- Midwest (Chicago, Kansas City)
- Southwest (Dallas)
- Rocky Mountain (Denver)
- Pacific (San Francisco, Los Angeles, Seattle)

What Is the Office for Civil Rights (OCR)?

Pacific Region covers the following states:

- Alaska
- Arizona
- California
- Hawaii
- Idaho
- Nevada
- Oregon
- Washington
- U.S. Pacific Territories

Enforcement and Compliance Activities

- Complaint Investigations
- OCR Complaint portal
- Compliance Reviews
- Voluntary Resolution Agreements
- Formal Enforcement
- Audits
- Outreach and Public Education
- Policy Development

Filing Complaints

- Any person or organization may file a complaint with OCR by mail or electronically
  - Only for possible violations occurring after compliance date of the law at issue
  - Complaints should be filed within 180 days of when the complainant knew or should have known that the act or omission occurred
- Individuals may also file complaints with Covered Entities

Complaint Process

- Informal review may resolve issue fully without formal investigation
  - Many complaints will be resolved at this stage
- If not, begin investigation
  - Voluntary resolution may be possible through
    - Education
    - Training
- Technical Assistance
- Some cases may require formal enforcement

Major Laws Enforced By OCR

- Title VI of the Civil Rights Act of 1964
- Section 504 of the Rehabilitation Act of 1973
- Title II of the Americans with Disabilities Act of 1990
- The Age Discrimination Act of 1975
- Section 1557 of the Affordable Care Act
- Health Insurance Portability and Accountability Act of 1996 (HIPAA Privacy, Security, and Breach Notification Rules)

Establishing Civil Rights Jurisdiction

Establishing Jurisdiction

- Does OCR have subject matter jurisdiction?
  - Does the complaint allege discrimination or retaliation on a basis prohibited by one of the statutes or regulations that OCR is responsible for enforcing?
- Does OCR have jurisdiction over the entity named in the complaint?
  - Do we have jurisdiction over the program, activity, or entity alleged to have engaged in discrimination?

Jurisdiction over the Entity

- Depending on the statute at issue, OCR has Federal civil rights jurisdiction over:
  - Programs and activities that receive Federal financial assistance (FFA) from HHS
  - Federally (HHS) conducted programs
  - Public entities (state or local governments)
  - Covered entities under Section 1557

What is Federal Financial Assistance (FFA)?

- "Federal financial assistance" means assistance in the form of any grant, loan, or contract.

- See 42 U.S.C. § 2000d-1

Examples of FFA Recipients in the OCR Context

- Health care providers participating in CHIP and Medicaid programs
- Hospitals and nursing homes that accept Medicare Part A
- Medicare Advantage Plans (HMOs and PPOs) under Medicare Part C
- Prescription Drug Plan sponsors and Medicare Advantage Drug Plans under Medicare Part D
- Head Start Programs
- TANF Programs
- Adoption and Foster Care Agencies
- Scholarships, loans, and grants are also FFA

OCR's Civil Rights Authorities

Title VI of the Civil Rights Act of 1964

Prohibits discrimination in programs receiving FFA on the basis of:

- Race
- Color
- National origin

Section 504 of the Rehabilitation Act of 1973

Prohibits discrimination on the basis of disability in:

- Programs and activities that receive FFA
- Federally conducted programs (HHS)

The Americans with Disabilities Act (ADA)

- Passed in 1990
- Comprehensive law which applies Section 504 prohibitions to the private sector as well as state and local governments
- Contains 5 titles and is enforced by a variety of federal agencies

Title II of the ADA

- HHS enforces Title II which deals with state and local government agencies
- Employs the same concepts as used in Section 504: integration, equal and effective, modification, program accessibility
- FFA does not have to be established to assert ADA, Title II jurisdiction

Section 1557 of the Affordable Care Act (ACA)

- Prohibits discrimination on the basis of race, color, national origin, disability, age, or **sex** in any health program or activity that
  - receives financial assistance from HHS.
  - is administered by an HHS agency or any entity established under Title I of ACA.
    - Extends nondiscrimination protections to the Marketplaces

Sex Discrimination under Section 1557

- Includes discrimination on the basis of:
  - Sex
  - Gender identity/expression
    - Including transgender status
  - Nonconformity to sex stereotypes
    - i.e. to traditional concepts of masculinity or femininity
  - OCR has already received many complaints in this area (sex discrimination).

Title IX of the Education Amendments Act of 1972

- Prohibits discrimination on basis of sex in all educational and training programs operated by a recipient of FFA

- OCR has limited jurisdiction under Title IX
  - Example: where a State Department of Human Services receiving FFA from HHS provides a class for new fathers, but not for new mothers

OCR's Health Information Privacy Authorities

Overview of the Privacy, Security, and Breach Notification Rules

HIPAA Privacy Rule

2003 - Subpart E of HIPAA

45 CFR §§164.500-164.534

Scope: Who is Covered?

- Limited by HIPAA to:
  - "Covered Entities" (CEs):
    - 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 Associates

§160.103

Business Associates (BA)

- Agents, contractors, and others hired to do the work of, or to work for, the CE, and such work requires the use or disclosure of protected health information (PHI).
  - A BA expressly includes Health Information Organizations, E-prescribing Gateways, and PHR vendors that provide services to covered entities. Subcontractors of a BA are also defined as a BA.
  - BAs are directly liable for certain violations of the Privacy, Security, and Breach Notification Rules.
- The Privacy Rule requires "satisfactory assurance," in the form of a contract (or Business Associate Agreement), 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 Covered Entities or their Business Associates
- Not PHI:
  - De-identified information (per Safe Harbor or expert method)
  - 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 (or his/her personal representative) who is the subject of the PHI.
  - To the Secretary of HHS to determine compliance.
- All other uses and disclosures in the Privacy Rule are *permissive.*
- Covered Entities may provide greater protections.

§164.502

Permissive Uses and Disclosures

- For treatment, payment, and health care operations (TPO)
- With the individual's opportunity to agree or object
- For specific public priorities (e.g., public health or where required by law)
- "Incident to" a permitted use or disclosure
- Limited data sets
- As authorized by the individual

§164.502

HIPAA Security Rule

2005 - Subpart C of HIPAA

45 CFR §§ 164.302-164.318

Definitions & General Rules

- General Rules
  - Establishes the requirements CEs and BAs must meet
  - Includes the consideration for a flexibility of approach
  - Defines the required standards and implementation specifications (both required and addressable)
  - Requires maintenance of security measures implemented to support the reasonable and appropriate protection of **electronic** protected health information (ePHI)

HHS Approach to HIPAA Security

- Standards to assure the confidentiality, integrity, and availability of ePHI
- Through reasonable and appropriate safeguards
- Addressing vulnerabilities identified through analysis and management of risk
- Appropriate to the size and complexity of the organization and its information systems
- Technology neutral

Scope: What is Covered?

- Applies to Electronic Protected Health Information (e-PHI) that a Covered Entity or a Business Associate:
  - Creates
  - Receives
  - Maintains
  - Transmits
- Electronic vs. Oral and Paper PHI
  - Privacy Rule applies to all forms of PHI
  - Security Rule applies only to e-PHI

Breach Notification

2009 and 2013 – Subpart D of HIPAA

45 CFR §§ 164.400-164.414

Brief Summary

- Covered entities must:
  - Notify each affected individual of breach of "unsecured protected health information."
  - Notice to media if more than 500 people affected.
  - Notice to Secretary of breach through OCR website.
  - Notifications to be provided without unreasonable delay (but no later than 60 days of discovery of breach).
- Business associates must notify covered entities of breach and identify individuals affected.

What is a “breach”?

- “Acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the Privacy Rule] which compromises the security or privacy of the protected health information.”
- Presumption of breach unless a covered entity or business associate can demonstrate a low probability that PHI has been compromised based on at least the following factors:
  - Nature and extent of PHI
  - The person who used or received the PHI
  - Whether PHI was actually viewed or acquired
  - Extent risk has been mitigated

HIV CR and HIPAA Enforcement Highlights

45 CFR Part 160, Subparts C, D, and E

HIV CR and HIPAA Enforcement Highlights

Massachusetts General Hospital Settles Potential HIPAA Violations:
The General Hospital Corporation and Massachusetts General Physicians Organization, Inc. (Mass General) has agreed to pay the U.S. government $1,000,000 to settle potential violations of the HIPAA Privacy Rule.

The incident giving rise to the agreement involved the loss of protected health information (PHI) of 192 patients of Mass General's Infectious Disease Associates outpatient practice, including patients with HIV/AIDS. OCR opened its investigation of Mass General after a complaint was filed by a patient whose PHI was lost on March 9, 2009. OCR's investigation indicated that Mass General failed to implement reasonable, appropriate safeguards to protect the privacy of PHI when removed from Mass General's premises and impermissibly disclosed PHI potentially violating provisions of the HIPAA Privacy Rule.

This impermissible disclosure involved the loss of documents consisting of a patient schedule containing names and medical record numbers for a group of 192 patients, and billing encounter forms containing the name, date of birth, medical record number, health insurer and policy number, diagnosis and name of providers for 66 of those patients..

HIV CR and HIPAA Enforcement Highlights

San Agustin:

Winston C. San Agustin, M.D is a California physician, who practices neurological surgery in Monterey Park, California. He participated in Medi-Cal. Because he participated in the Medi-Cal program, Dr. Agustin received federal financial assistance. As a recipient of federal financial assistance, he was prohibited from discriminating against any qualified handicapped person. Examples of "prohibited discriminatory actions" include denying an individual a service or other benefit provided under a program that receives federal financial assistance from the Department of Health and Human Services. Dr. Agustin violated Section 504 because he refused to provide medical services to an individual based on that person's disability by refusing to provide medical services solely because the individual was HIV-positive. Dr. Agustin's compliance with Section 504 could not be secured by voluntary means, and his receipt of federal financial assistance was terminated. Dr. San Agustin thereafter entered into a post- termination compliance agreement with OCR to ensure his compliance with Section 504.

HIV CR and HIPAA Enforcement Highlights

On July 14, 2016, OCR released a report on its National HIV/AIDS Compliance Review Initiative . This important Initiative was initiated in 2014 and 2015, when OCR conducted coordinated compliance reviews at 12 hospitals – one hospital in each of the 12 cities most impacted by HIV/AIDS: Atlanta, GA; Baltimore, MD; Chicago, IL; Dallas, TX; Houston, TX; Los Angeles, CA; Miami, FL; New York City, NY; Philadelphia, PA; San Francisco, CA; San Juan, PR; and Washington, DC.

OCR Web Site

- http://www.hhs.gov/ocr/hipaa/
- Full text of Privacy, Security, and Breach 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