United States Department of Health & Human Services

Office of the Secretary
Office for Civil Rights (OCR)

HIPAA Enforcement

Valerie Morgan-Alston, Esq.
Deputy Director of Enforcement and Regional Operations
Office for Civil Rights
U.S. Department of Health and Human Services

Nineteenth National HIPAA Summit
March 9, 2011

Your Health. Your Rights

- **OCR's Vision:**

  Through investigations, voluntary dispute resolution, enforcement, technical assistance, policy development and information services, OCR will protect the civil rights of all individuals who are subject to discrimination in health and human services programs and protect the health information privacy rights of consumers.

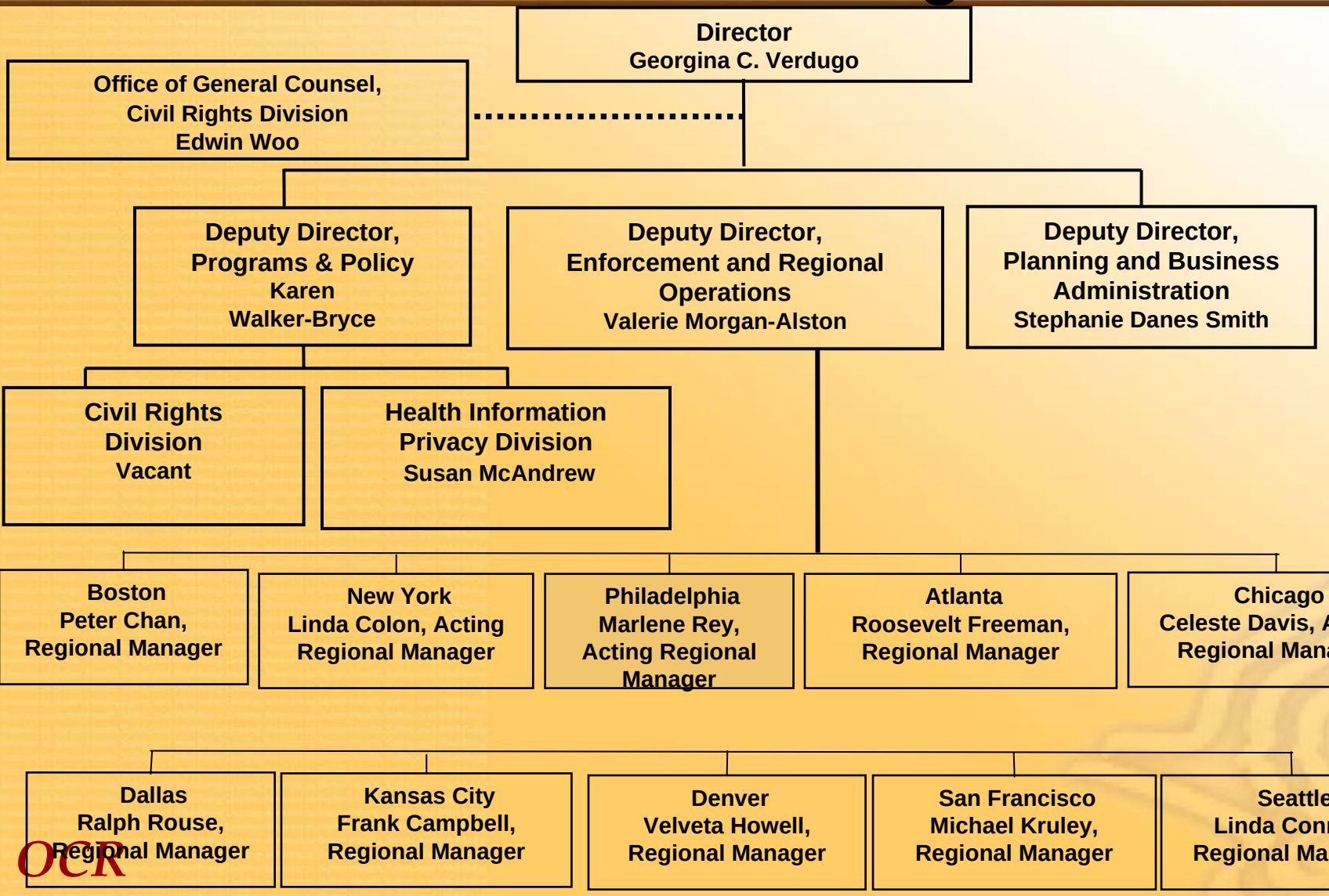
Who We Are

- **Headquarters:**
  - Policy
  - Administration
  - Case management and oversight
  - External relations

- **10 HHS regional offices:**
  - Enforcement
  - Investigation
  - Compliance reviews
  - Public education and outreach
  - Technical assistance

Department of Health and Human Services

Office for Civil Rights



OCR

Recent Enforcement Actions

HITECH has allowed the Secretary to impose significantly increased penalty amounts for violations of the HIPAA rules and encouraged prompt corrective action.

Implementation of HITECH Act enforcement has strengthened the HIPAA protections and rights related to an individual's health information.

This strengthened penalty scheme will encourage covered entities and business associates to comply with the HIPAA Privacy and Security and HITECH requirements.

Cignet Health Care

- Cignet Health Care is a treatment provider and health plan issuer
- Over a two-year period, 41 individuals complained to OCR that Cignet had ignored their requests for access to their health records
- Cignet failed to respond to OCR's investigation or provide copies of the patients' records

CMP of $4.3 Million Levied

- Civil Money Penalty of $1.3 million attributable to failure to provide individuals access to their health records

- Penalty of $3 million for failure to respond to OCR demands to produce records and failure to cooperate with OCR's investigation

Massachusetts General Hospital

- Large multi-specialty healthcare provider
- Employee, who had taken patient files home, left the folders on the subway train and they were never recovered
- Investigation initiated after media reports of incident and a complaint from an individual whose PHI was lost
- Settled with OCR through Resolution Agreement and corrective action plan

Actions to Settle Case

- $1 million resolution amount
- Corrective Action Plan
- MGH required to actively monitor its compliance with the Corrective Action Plan through use of an internal monitor

Management Services Organization of Washington

- MSO provided practice management services to individual health care providers
- Affiliated company, Washington Practice Management, markets and sells Medicare Advantage plans to consumers for which it earns commissions
- Separate agreements with DOJ and OIG to settle allegations under the Federal False Claims Act

Indications of Noncompliance WA MSO Resolution Agreement

- MSO disclosed ePHI to WPM, without a valid authorization, so that WPM could market Medicare Advantage plans to those individuals
- MSO had not developed or implemented appropriate and reasonable administrative, technical, and physical safeguards to protect ePHI

Actions to Settle Case

- $35,000 resolution amount to OCR
- Corrective Action Plan
  - Develop and implement policies & procedures to demonstrate compliance with the Privacy and Security Rules
  - Train workforce members
  - Conduct internal monitoring
  - Submit compliance reports to HHS for a period of two years

Rite Aid Corporation

- Large US pharmacy chain
- Series of media reports about personnel disposing of PHI, including labeled pill bottles and prescriptions, in unsecured garbage containers outside of several Rite Aid pharmacy stores
- Settled with OCR through Resolution Agreement and corrective action plan
- Simultaneously settled with FTC through a consent order

Indications of Non-Compliance in Rite Aid Resolution Agreement

- Rite Aid policies and procedures for disposal did not reasonably and appropriately safeguard PHI
- Rite Aid did not maintain sanctions policy for workforce members who failed to safeguard PHI in disposal process
- Rite Aid did not provide necessary and appropriate training for its workforce regarding disposal of PHI

Actions to Settle Case

- $1 million resolution amount
- Corrective Action Plan
- Both HHS and FTC require RAC to actively monitor its compliance with the Resolution Agreement and Consent Order

Actions to Settle Case

1. Revising, distributing policies & procedures regarding PHI disposal
2. Sanctioning workers who do not follow them
3. Training workforce members
4. Conducting internal monitoring
5. Engaging a third-party assessor to render reports to HHS
6. New internal reporting procedures requiring workers to report all violations of these new privacy policies and procedures
7. Submitting compliance reports to HHS for a period of three years

A Culture of Compliance

- In light of OCR's clearly articulated intention to aggressively enforce the HIPAA Privacy and Security Rules, covered entities and business associates should review their current HIPAA compliance programs.
- A robust compliance program includes employee training, vigilant implementation of policies and procedures, regular internal audits, and a prompt action plan to respond to incidents.

Want More Information?

The OCR website, http://www.hhs.gov/ocr/privacy/ offers a wide range of helpful information about health information privacy including educational information, FAQ's, and rule text and guidance for the Privacy, Security, and Breach Notification Rules.