U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Current State of HIPAA Enforcement

Abby Bonjean, Investigator
Office for Civil Rights, Midwest Region
May 6, 2016

1

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

These slides, along with Ms. Bonjean's remarks, are intended to be purely informational and informal in nature. None of the information contained in the slides or in Ms. Bonjean's statements is intended to represent or reflect the official interpretation or position of the U.S. Department of Health and Human Services, Office for Civil Rights.

2

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Today's Agenda

- Enforcement Basics
- Responding to OCR Inquiries
- Current State of Enforcement
  - Enforcement Statistics
  - Audit Program
  - Recent Enforcement Actions
- Common Compliance Issues
- Guidance and Compliance Tools

3

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

OCR Enforcement Basics

Types of OCR Inquiries

- Complaint Investigations
  - 45 C.F.R. § 160.306
- Compliance Reviews
  - 45 C.F.R. § 160.308

4

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

OCR Enforcement Basics

Overview of Investigative Process

- Notification and Data Request
- Covered Entity/Business Associate Response
  - 45 C.F.R. § 160.310 outlines responsibilities
- On-site Investigation
- Case Resolution
  - No Violation or Voluntary Compliance
  - Resolution Agreement (RA) and Corrective Action Plan (CAP)
  - Civil Money Penalty (CMP)

5

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Responding to OCR Inquiries

6

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Information OCR Often Requests

- Name and contact information of individual designated to work with OCR
- Position statement
- Business Associate Agreement (if applicable)
- Policies and procedures
- Evidence of workforce training
  - Training materials
  - Workforce attendance
- Evidence of sanctions (if applicable)

7

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Information OCR Often Requests (cont.)

- Security Rule cases
  - Risk analysis
  - Risk management plan
    - Evidence of implemented security measures
  - Security incident report
- Breach cases
  - Notices to individuals and media
  - Evidence of corrective action

8

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Preparing the Response

- Ask questions
- Response format
- Evidence = documentation
- Be forthcoming

9

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Current State of Enforcement

10

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

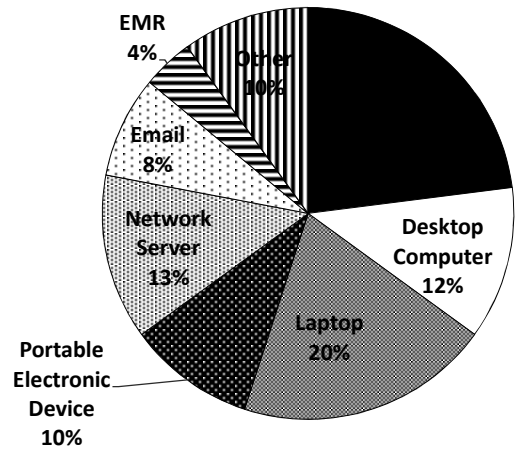
Enforcement Statistics

- CY 2015 Resolution Agreements/Corrective Action Plans
  - 6 RA/CAPs
  - Total resolution amounts of $6,193,400
- Breach Reports as of March 2, 2016
  - 1,476 reports involving 500 or more individuals
  - Over 222,000 reports involving fewer than 500 individuals

11

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

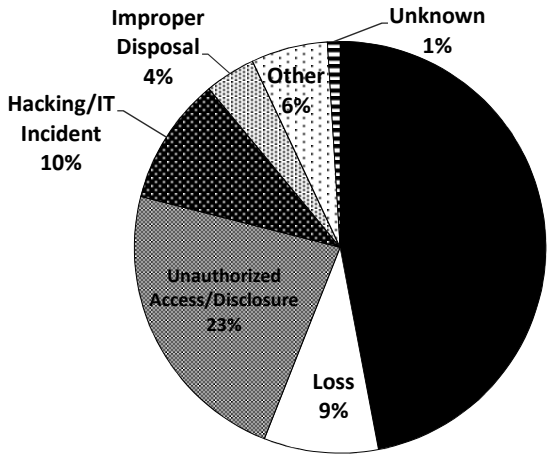
Breach Notification: 500+ Breaches by Location of Breach



12

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Breach Notification: 500+ Breaches by Type of Breach



13

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Audit Program

- Using FCi Federal contractors to help support next phase
- Verifying contact information for CEs and BAs
- Next round mostly desk audits
- Additional information on OCR's website
  - Revised protocol

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html

14

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Recent Enforcement Actions

- New York Presbyterian ($2.2 million)
  - Disclosed PHI to film crew and staff of the television series "NY Med," without authorization
  - Violations:
    - Impermissible Disclosure
    - Safeguards
- Raleigh Orthopaedic Clinic ($750,000)
  - Disclosed PHI to third party vendor without obtaining satisfactory assurances in the form of written business associate agreement
  - Violations:
    - Impermissible Disclosure
    - Business Associate Agreement

15

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Recent Enforcement Actions

- Feinstein Institute for Medical Research ($3.9 million)
  - Researcher failed to safeguard laptop containing patient and research participant ePHI
  - Violations:
    - Risk Analysis
    - Access Authorization
    - Workstation Security
    - Device and Media Controls
    - Encryption
    - Impermissible Disclosure
- North Memorial Health Care ($1,550,000)
  - Breach by business associate, Accretive
  - Violations:
    - Risk Analysis
    - Business Associate Agreement
    - Impermissible Disclosure

16

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Recent Enforcement Actions

- Complete PT ($25,000)
  - Posting of PHI on website without patient authorization
  - Violations:
    - Impermissible Disclosure
    - Safeguards
    - Privacy Rule Policies and Procedures
- Lincare ($239,800)
  - PHI of 278 patients removed from company office, left exposed and then abandoned altogether
  - Violations:
    - Impermissible Disclosure
    - Safeguards
    - Privacy Rule Policies and Procedures

17

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Recent Enforcement Actions

- University of Washington Medicine ($750,000)
  - Malware compromised IT system and ePHI of approximately 90,000 individuals
  - Violation:
    - Risk Analysis
- Triple-S Management Corporation ($3.5 million)
  - Multiple breaches
  - Violations:
    - Risk Analysis
    - Risk Management
    - Termination Procedures
    - Business Associate Agreement
    - Impermissible Disclosure
    - Minimum Necessary
    - Safeguards

18

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Recent Enforcement Actions

- Lahey Hospital and Medical Center ($850,000)
  - Theft of laptop containing ePHI of 599 individuals from stand that accompanied portable CT scanner
  - Violations:
    - Risk Analysis
    - Workstation Security
    - Device and Media Controls
    - Unique User Identification
    - Audit Controls
    - Impermissible Disclosure

19

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Recent Enforcement Actions

- Cancer Care Group ($750,000)
  - Unencrypted backup media containing the ePHI of approximately 55,000 individuals stolen from a workforce member's car
  - Violations:
    - Risk Analysis
    - Device and Media Controls
    - Impermissible Disclosure
- St. Elizabeth Medical Center ($218,400)
  - Internet-based document sharing application used to store ePHI
  - Separate breach involving laptop and USB drive
  - Violations:
    - Risk Management
    - Response and Reporting
    - Impermissible Disclosure (2)

20

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Common Compliance Issues

- Risk Analysis
  - Identify all ePHI
  - Ongoing process
- Risk Management
- Mobile Devices
  - Implement a policy
  - Train workforce members

21

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Common Compliance Issues

Addressable does not mean optional

- Refer to 45 C.F.R. § 164.306(d)(3)
  - Assess whether the implementation specification is reasonable and appropriate
    - If reasonable and appropriate, implement the measure
    - If not, document rationale and implement equivalent alternative measure

22

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Common Compliance Issues

Policies and Procedures

- 45 C.F.R. §§ 164.316, 164.414, 164.530(i)-(j)
- Revise as necessary to comply with applicable law and to address changes in business and workflow
- Should reflect an entity's environment

23

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Guidance and Compliance Tools

- Access Guidance
  http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html#newlyreleasedfaqs
- NIST Cybersecurity Framework
  http://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html
- HIT Developer Portal
  http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/samesexmarriage/index.html
- ONC Blog Posts on Interoperability
  https://www.healthit.gov/buzz-blog/category/privacy-and-security-of-ehrs/the-real-hipaa/
- Revised Guide to Privacy and Security of Electronic Health Information
  http://www.healthit.gov/providers-professionals/guide-privacy-and-security-electronic-health-information

24

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Guidance and Compliance Tools

- Sample Business Associate Contract Language
  http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
- Security Rule Guidance
  - Risk Analysis Guidance
    http://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html
  - NIST HIPAA Security Rule Toolkit
  - NIST Guidelines for Media Sanitation
  - FTC Guidance on Copier Data Security
    http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

25

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Guidance and Compliance Tools: www.healthit.gov/mobiledevices


Use a password or other user authentication.


Install and enable encryption.


Install and activate wiping and/or remote disabling.


Disable and do not install file-sharing applications.


Install and enable a firewall.


Install and enable security software.


Keep security software up to date.


Research mobile apps before downloading.


Maintain physical control of your mobile device.


Use adequate security to send or receive PHI over public Wi-Fi networks.


Delete all stored health information before discarding or reusing the mobile device.

26

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

In Development

- Cloud Computing Guidance
- ANPRM to solicit views on ways in which an individual who is harmed by an offense punishable under HIPAA may receive a percentage of any civil money penalty or monetary settlement collected

27

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Contact Information

Abby.Bonjean@hhs.gov
(312) 886-5895

Sign up for OCR's listserv:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/listserv.html

28