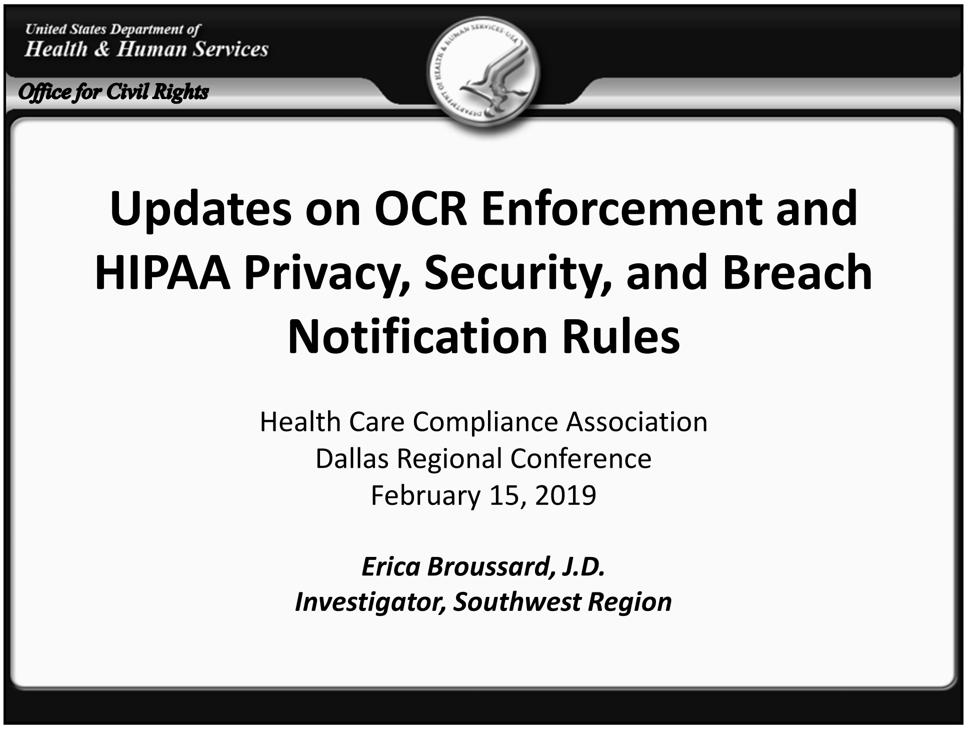
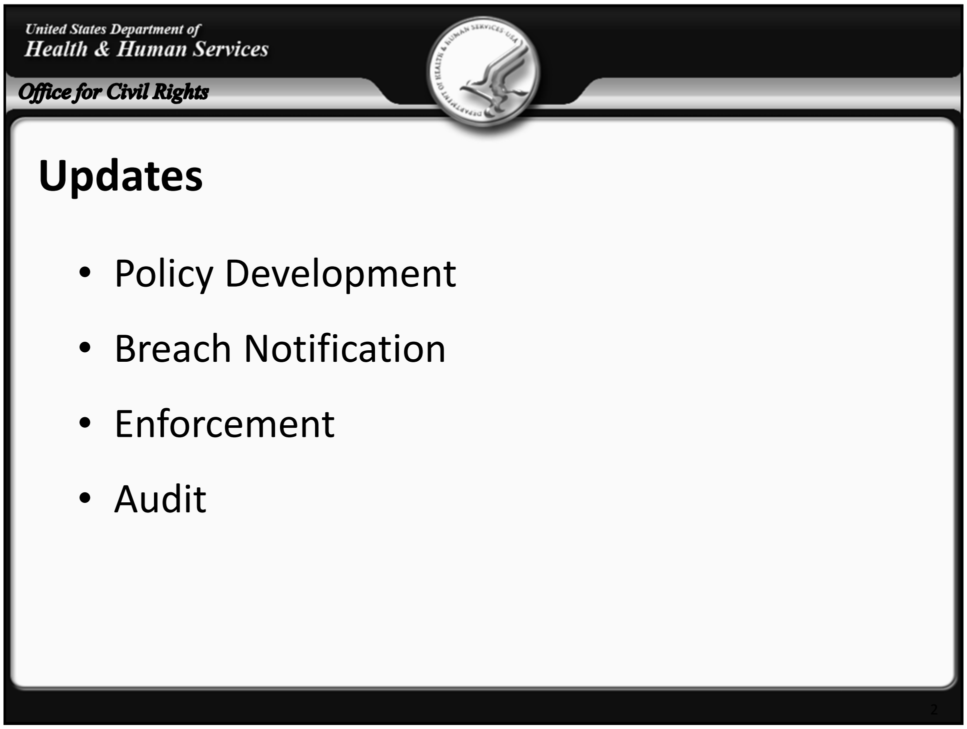


Updates on OCR Enforcement and HIPAA Privacy, Security, and Breach Notification Rules

Health Care Compliance Association
Dallas Regional Conference
February 15, 2019

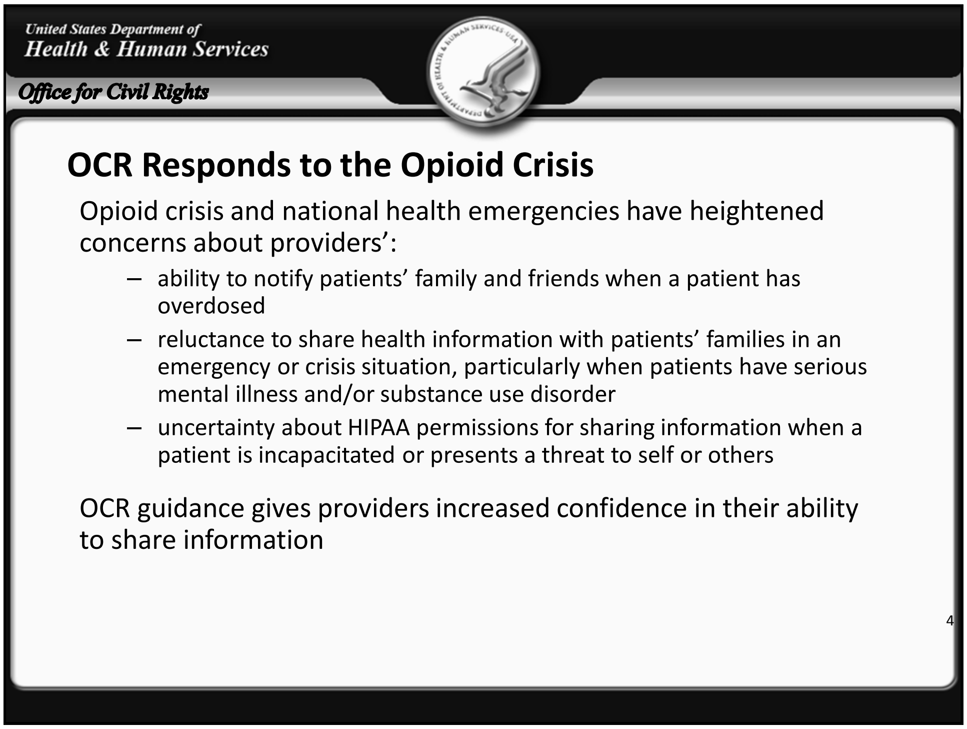
Erica Broussard, J.D.
Investigator, Southwest Region



Updates

- Policy Development
- Breach Notification
- Enforcement
- Audit

POLICY DEVELOPMENT

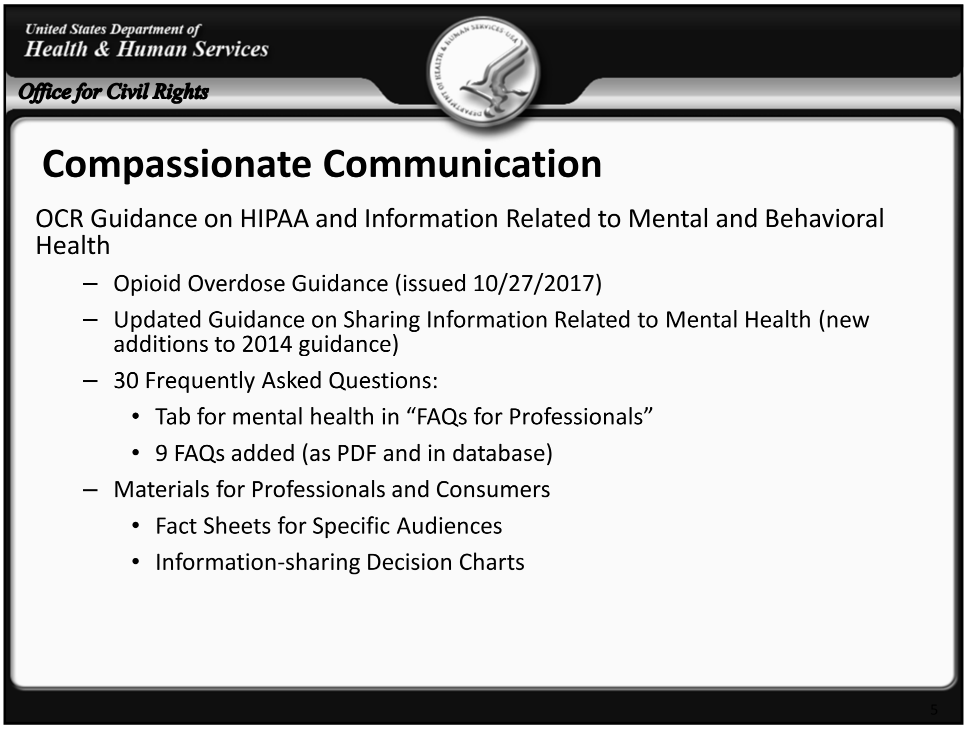


OCR Responds to the Opioid Crisis

Opioid crisis and national health emergencies have heightened concerns about providers':

- ability to notify patients' family and friends when a patient has overdosed
- reluctance to share health information with patients' families in an emergency or crisis situation, particularly when patients have serious mental illness and/or substance use disorder
- uncertainty about HIPAA permissions for sharing information when a patient is incapacitated or presents a threat to self or others

OCR guidance gives providers increased confidence in their ability to share information



United States Department of
Health & Human Services

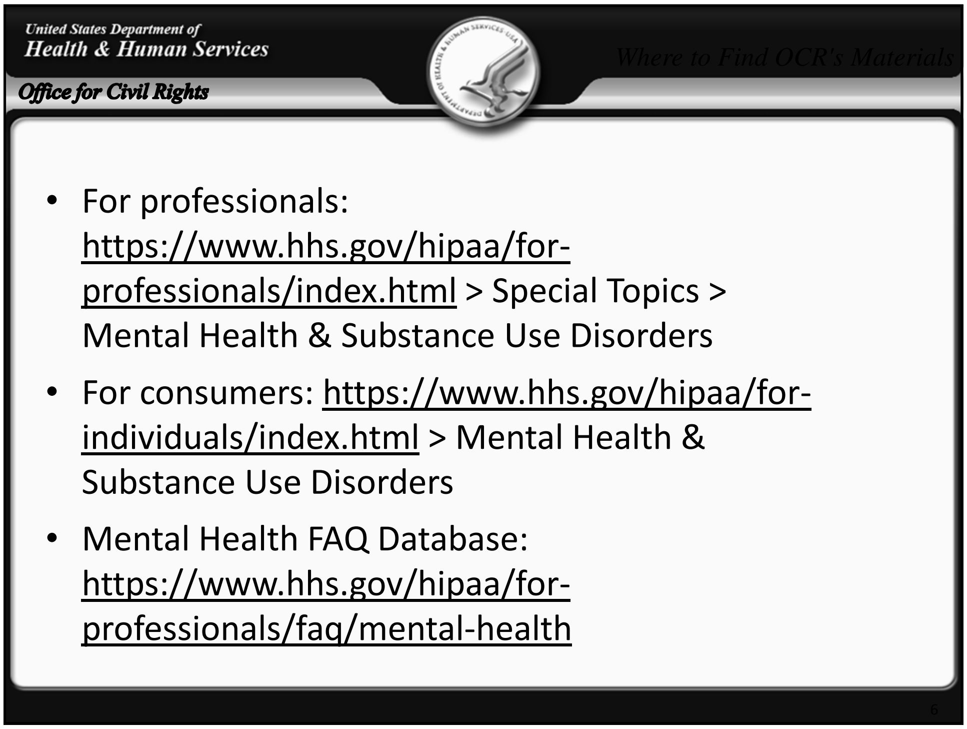
Office for Civil Rights

Compassionate Communication

OCR Guidance on HIPAA and Information Related to Mental and Behavioral Health

- Opioid Overdose Guidance (issued 10/27/2017)
- Updated Guidance on Sharing Information Related to Mental Health (new additions to 2014 guidance)
- 30 Frequently Asked Questions:
  - Tab for mental health in “FAQs for Professionals”
  - 9 FAQs added (as PDF and in database)
- Materials for Professionals and Consumers
  - Fact Sheets for Specific Audiences
  - Information-sharing Decision Charts

5



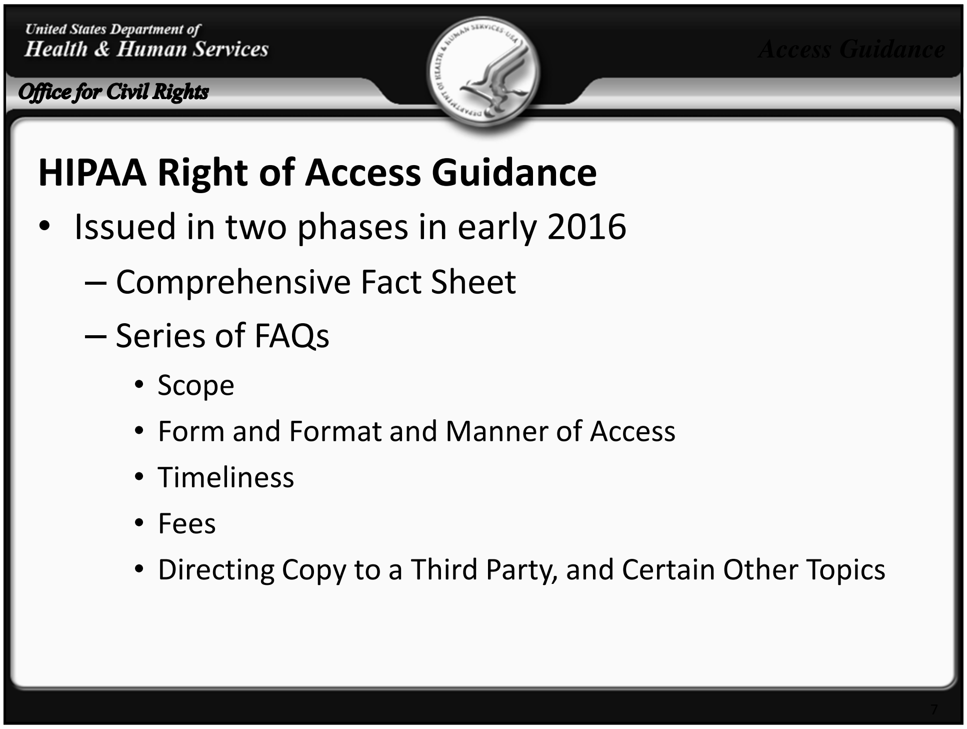
United States Department of
Health & Human Services

Office for Civil Rights

Where to Find OCR's Materials

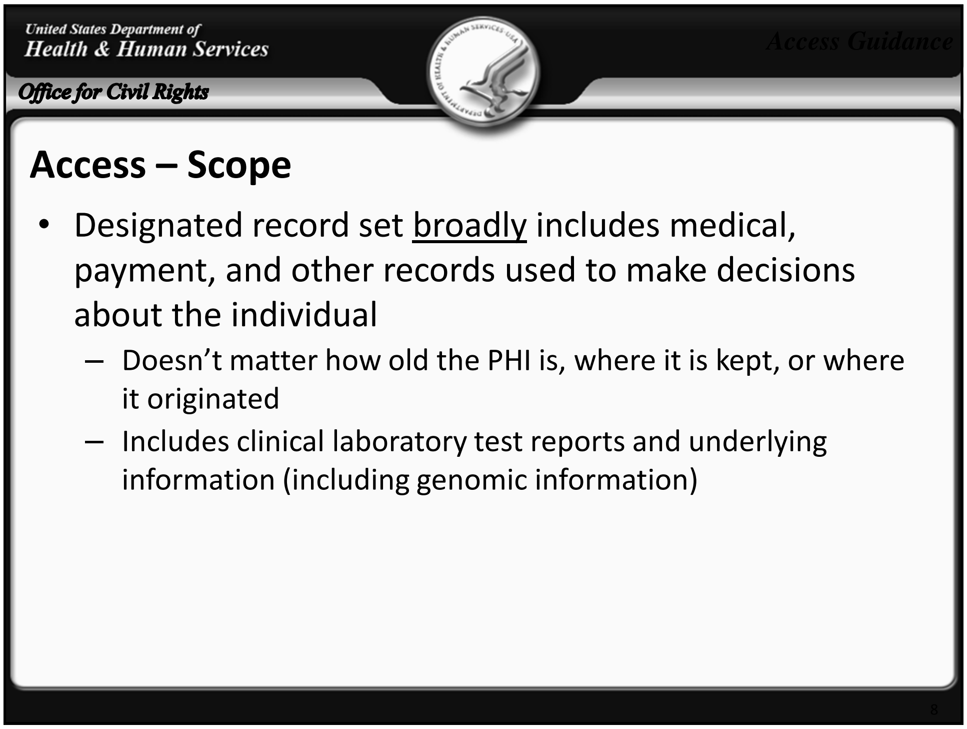
- For professionals: https://www.hhs.gov/hipaa/for-professionals/index.html > Special Topics > Mental Health & Substance Use Disorders
- For consumers: https://www.hhs.gov/hipaa/for-individuals/index.html > Mental Health & Substance Use Disorders
- Mental Health FAQ Database: https://www.hhs.gov/hipaa/for-professionals/faq/mental-health

6



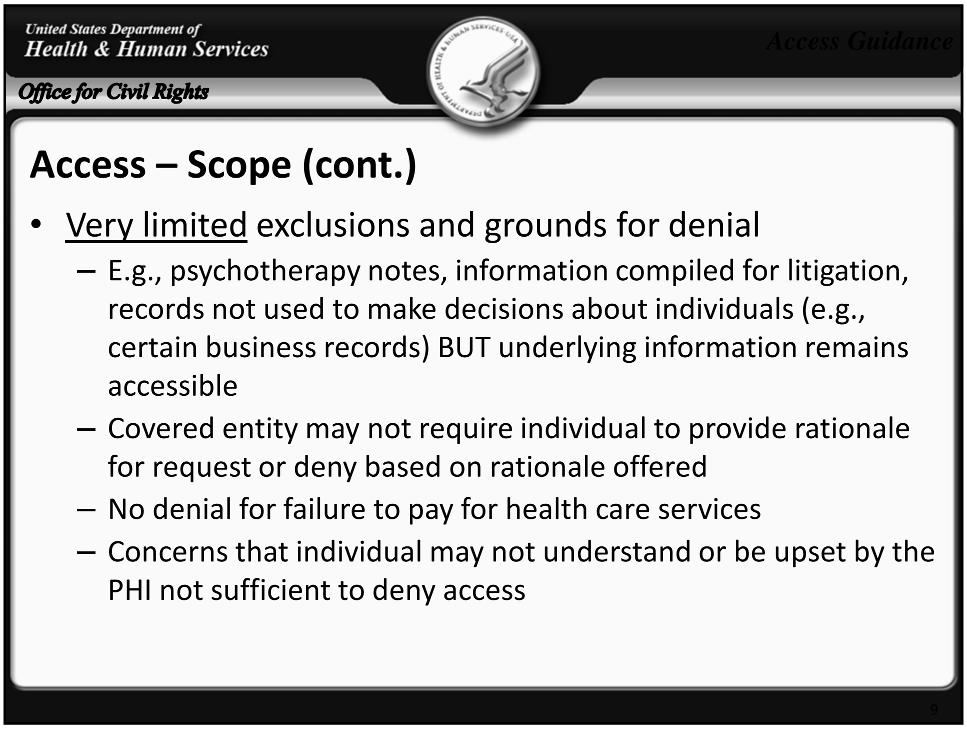
HIPAA Right of Access Guidance

- Issued in two phases in early 2016
  - Comprehensive Fact Sheet
  - Series of FAQs
    - Scope
    - Form and Format and Manner of Access
    - Timeliness
    - Fees
    - Directing Copy to a Third Party, and Certain Other Topics



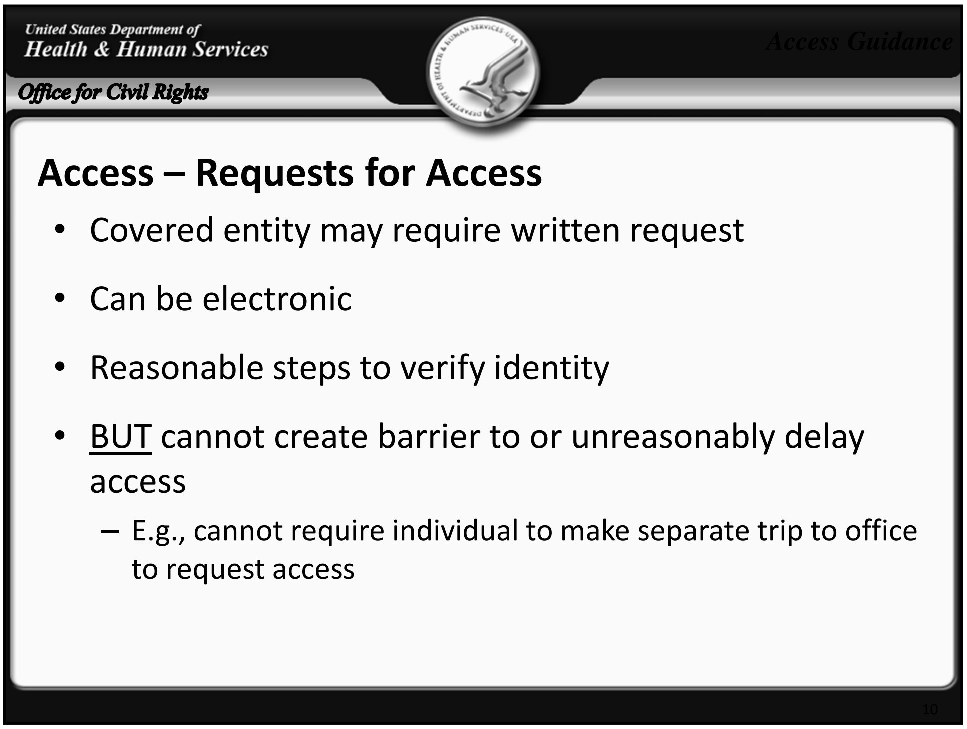
Access – Scope

- Designated record set broadly includes medical, payment, and other records used to make decisions about the individual
  - Doesn’t matter how old the PHI is, where it is kept, or where it originated
  - Includes clinical laboratory test reports and underlying information (including genomic information)



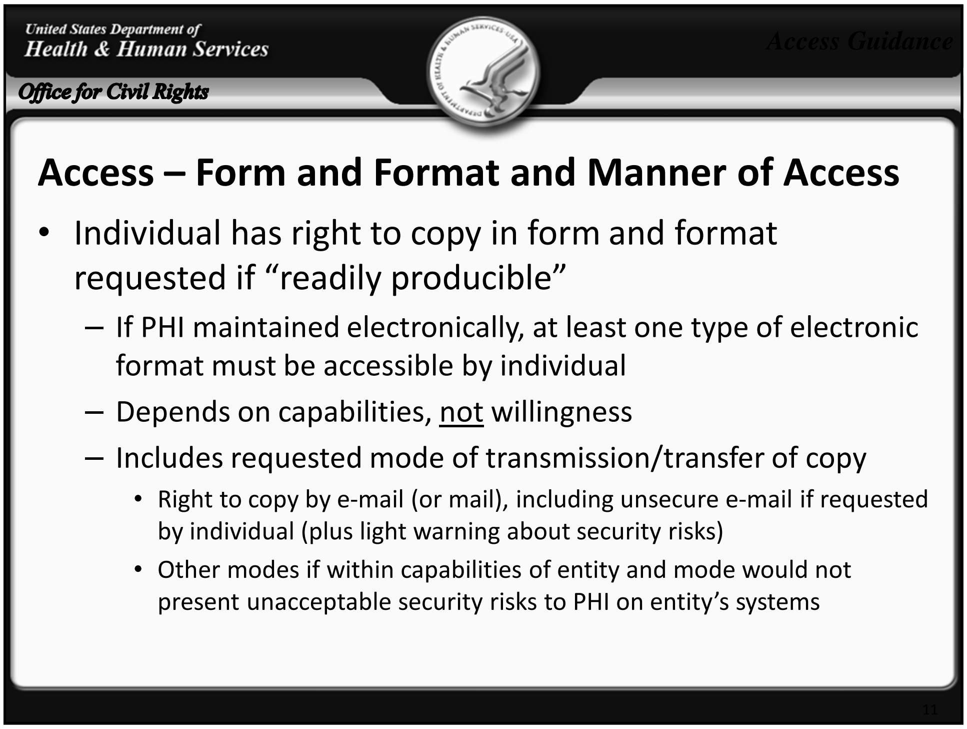
Access – Scope (cont.)

- Very limited exclusions and grounds for denial
  - E.g., psychotherapy notes, information compiled for litigation, records not used to make decisions about individuals (e.g., certain business records) BUT underlying information remains accessible
  - Covered entity may not require individual to provide rationale for request or deny based on rationale offered
  - No denial for failure to pay for health care services
  - Concerns that individual may not understand or be upset by the PHI not sufficient to deny access



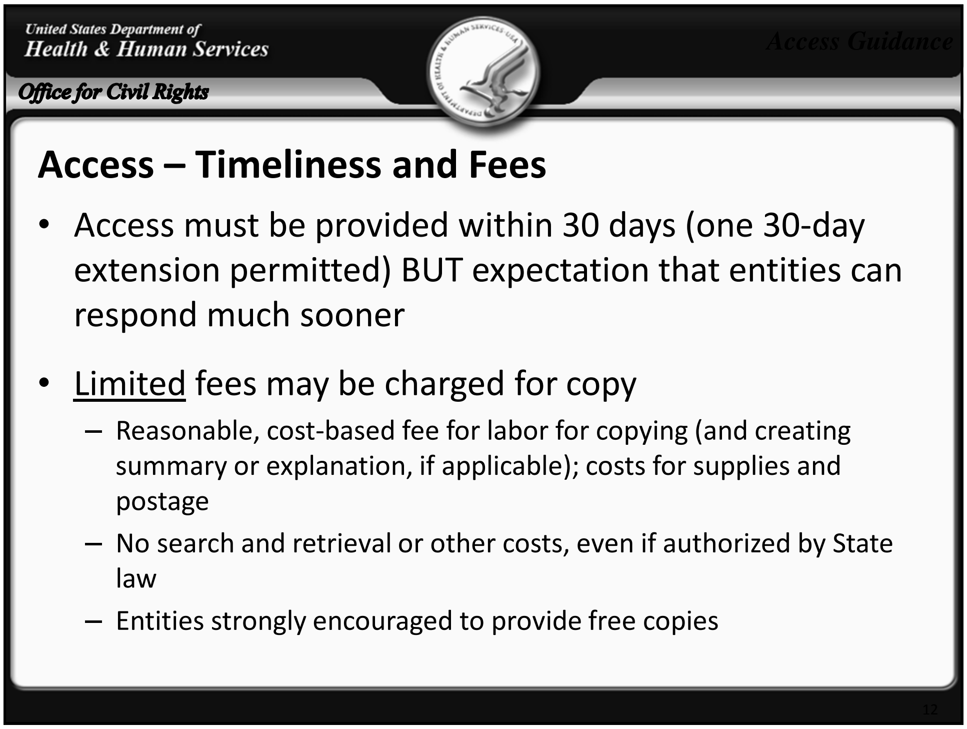
Access – Requests for Access

- Covered entity may require written request
- Can be electronic
- Reasonable steps to verify identity
- BUT cannot create barrier to or unreasonably delay access
  - E.g., cannot require individual to make separate trip to office to request access



Access – Form and Format and Manner of Access

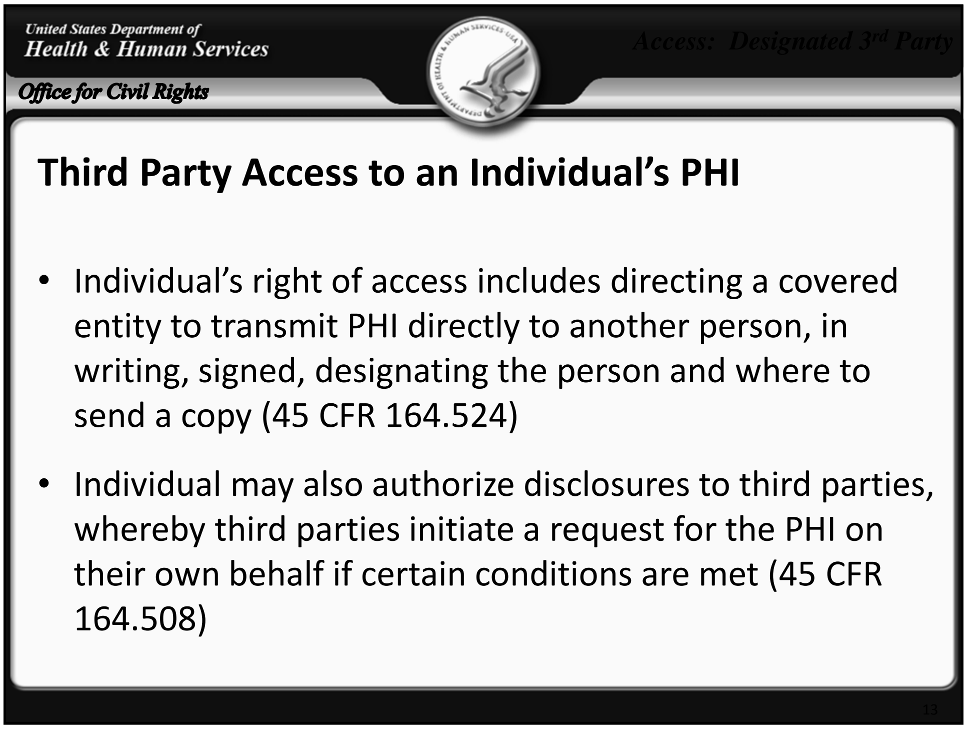
- Individual has right to copy in form and format requested if "readily producible"
  - If PHI maintained electronically, at least one type of electronic format must be accessible by individual
  - Depends on capabilities, not willingness
  - Includes requested mode of transmission/transfer of copy
    - Right to copy by e-mail (or mail), including unsecure e-mail if requested by individual (plus light warning about security risks)
    - Other modes if within capabilities of entity and mode would not present unacceptable security risks to PHI on entity's systems



Access – Timeliness and Fees

- Access must be provided within 30 days (one 30-day extension permitted) BUT expectation that entities can respond much sooner

- Limited fees may be charged for copy
  - Reasonable, cost-based fee for labor for copying (and creating summary or explanation, if applicable); costs for supplies and postage
  - No search and retrieval or other costs, even if authorized by State law
  - Entities strongly encouraged to provide free copies



United States Department of
Health & Human Services

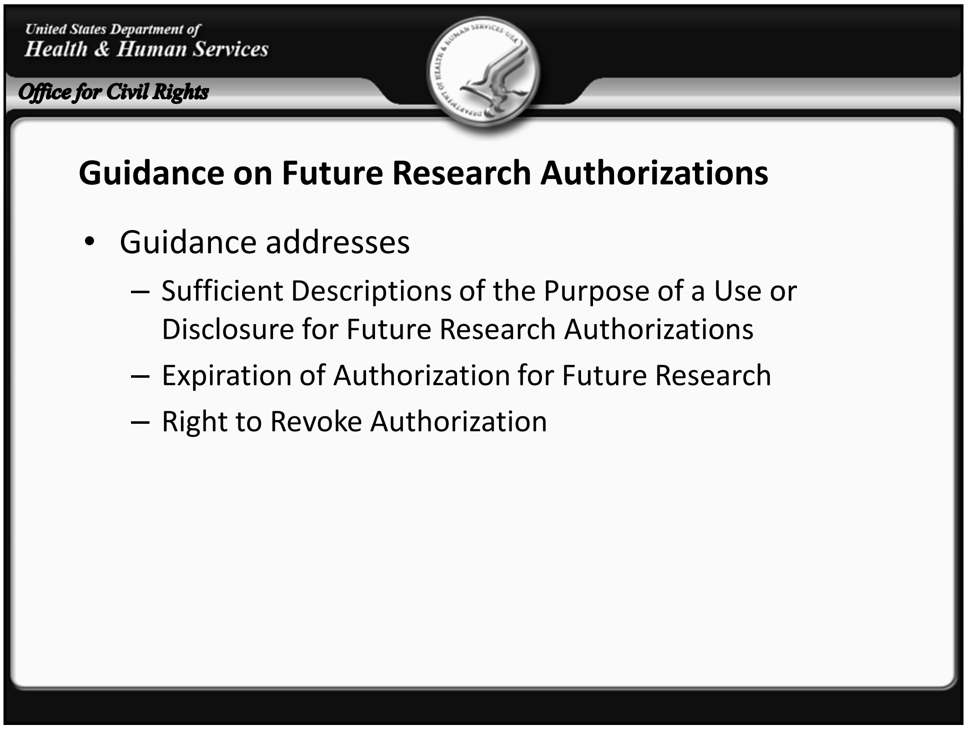
Office for Civil Rights

Access: Designated 3rd Party

Third Party Access to an Individual's PHI

- Individual's right of access includes directing a covered entity to transmit PHI directly to another person, in writing, signed, designating the person and where to send a copy (45 CFR 164.524)
- Individual may also authorize disclosures to third parties, whereby third parties initiate a request for the PHI on their own behalf if certain conditions are met (45 CFR 164.508)

13

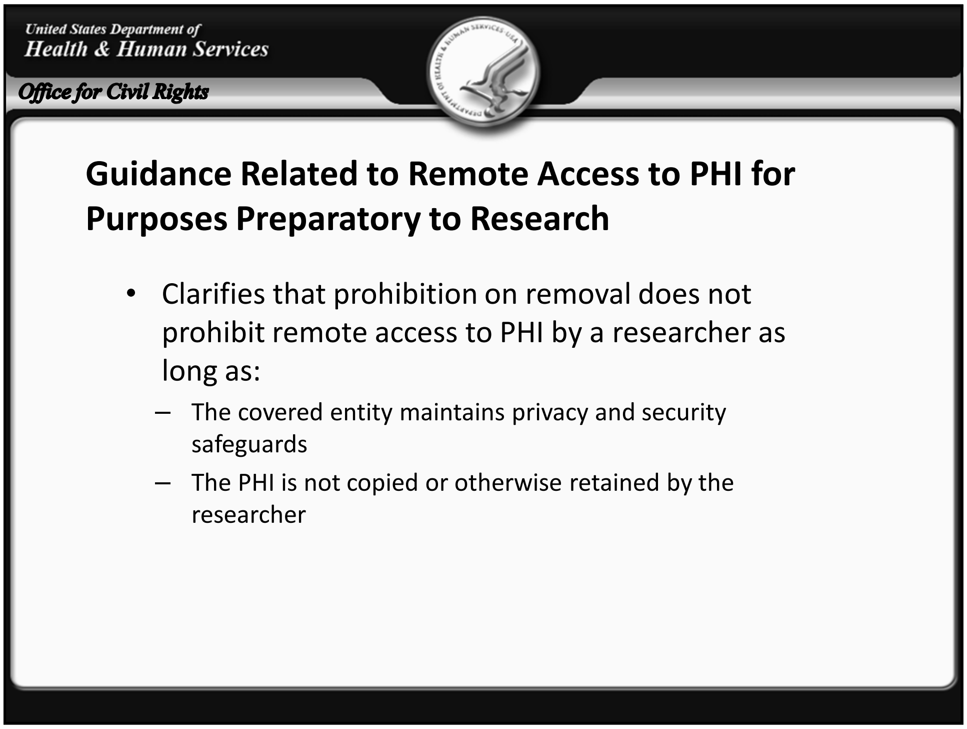


United States Department of
Health & Human Services

Office for Civil Rights

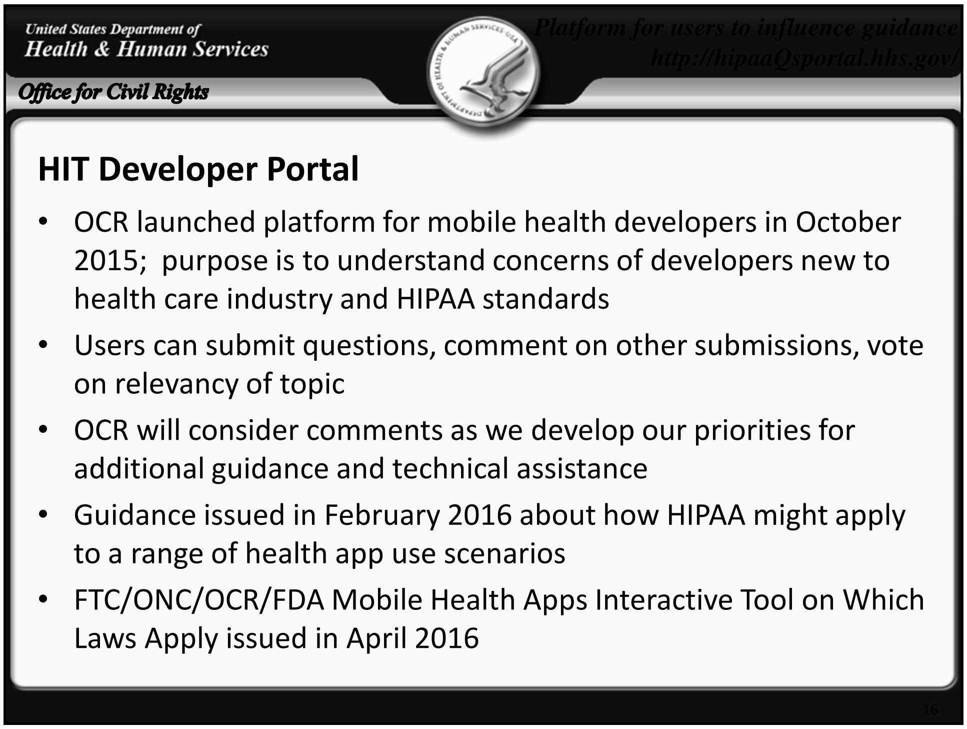
Guidance on Future Research Authorizations

- Guidance addresses
  - Sufficient Descriptions of the Purpose of a Use or Disclosure for Future Research Authorizations
  - Expiration of Authorization for Future Research
  - Right to Revoke Authorization



Guidance Related to Remote Access to PHI for Purposes Preparatory to Research

- Clarifies that prohibition on removal does not prohibit remote access to PHI by a researcher as long as:
  - The covered entity maintains privacy and security safeguards
  - The PHI is not copied or otherwise retained by the researcher

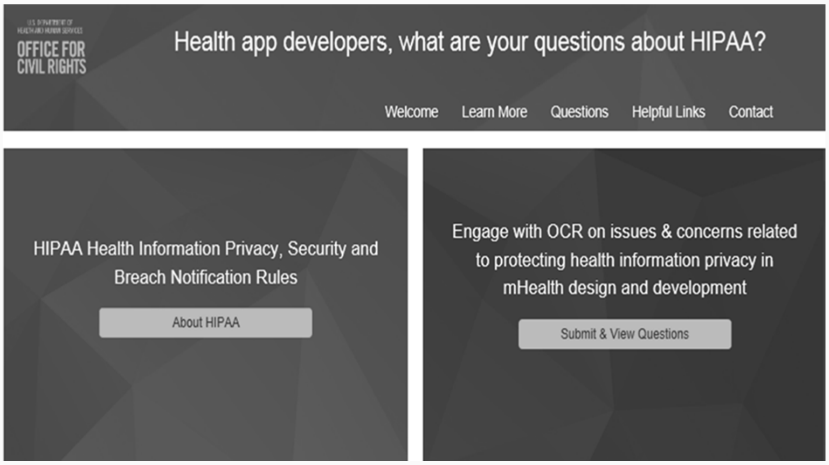


Platform for users to influence guidance
http://hipaaQsportal.hhs.gov/

HIT Developer Portal

- OCR launched platform for mobile health developers in October 2015; purpose is to understand concerns of developers new to health care industry and HIPAA standards
- Users can submit questions, comment on other submissions, vote on relevancy of topic
- OCR will consider comments as we develop our priorities for additional guidance and technical assistance
- Guidance issued in February 2016 about how HIPAA might apply to a range of health app use scenarios
- FTC/ONC/OCR/FDA Mobile Health Apps Interactive Tool on Which Laws Apply issued in April 2016

Platform for users to influence guidance http://hipaaQsportal.hhs.gov/



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

Health app developers, what are your questions about HIPAA?

HIPAA Health Information Privacy, Security and Breach Notification Rules

Engage with OCR on issues & concerns related to protecting health information privacy in mHealth design and development

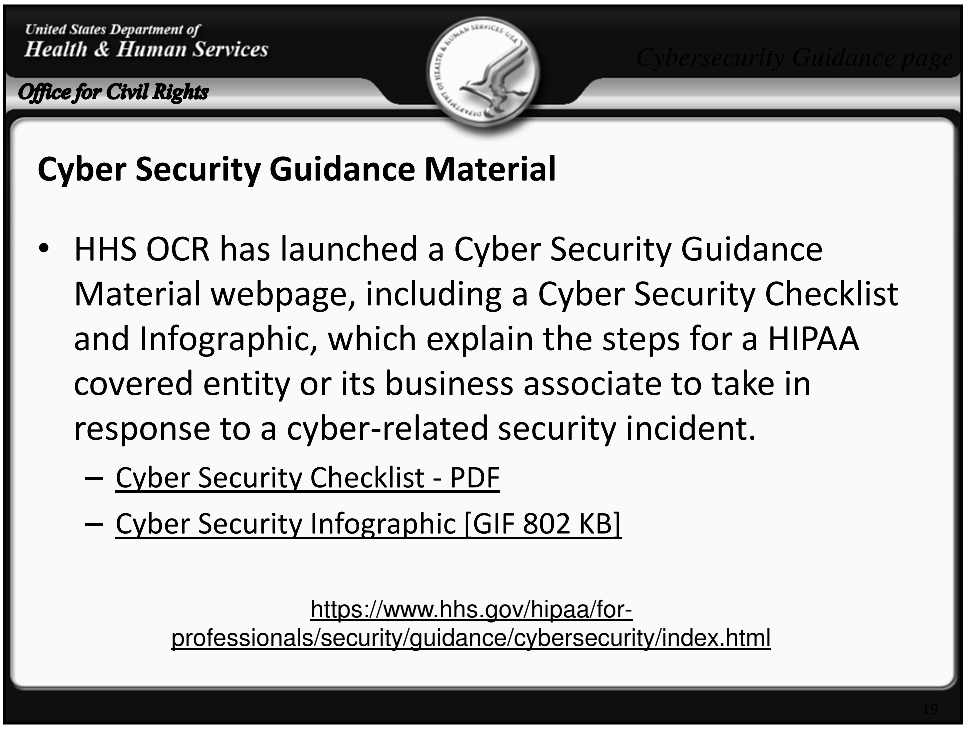
Cloud Guidance

Cloud Computing Guidance

- OCR released guidance clarifying that a CSP is a business associate – and therefore required to comply with applicable HIPAA regulations – when the CSP creates, receives, maintains or transmits identifiable health information (referred to in HIPAA as electronic protected health information or ePHI) on behalf of a covered entity or business associate.

- When a CSP stores and/or processes ePHI for a covered entity or business associate, that CSP is a business associate under HIPAA, even if the CSP stores the ePHI in encrypted form and does not have the key.

- CSPs are not likely to be considered “conduits,” because their services typically involve storage of ePHI on more than a temporary basis.
- http://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
- http://www.hhs.gov/hipaa/for-professionals/faq/2074/may-a-business-associate-of-a-hipaa-covered-entity-block-or-terminate-access/index.html



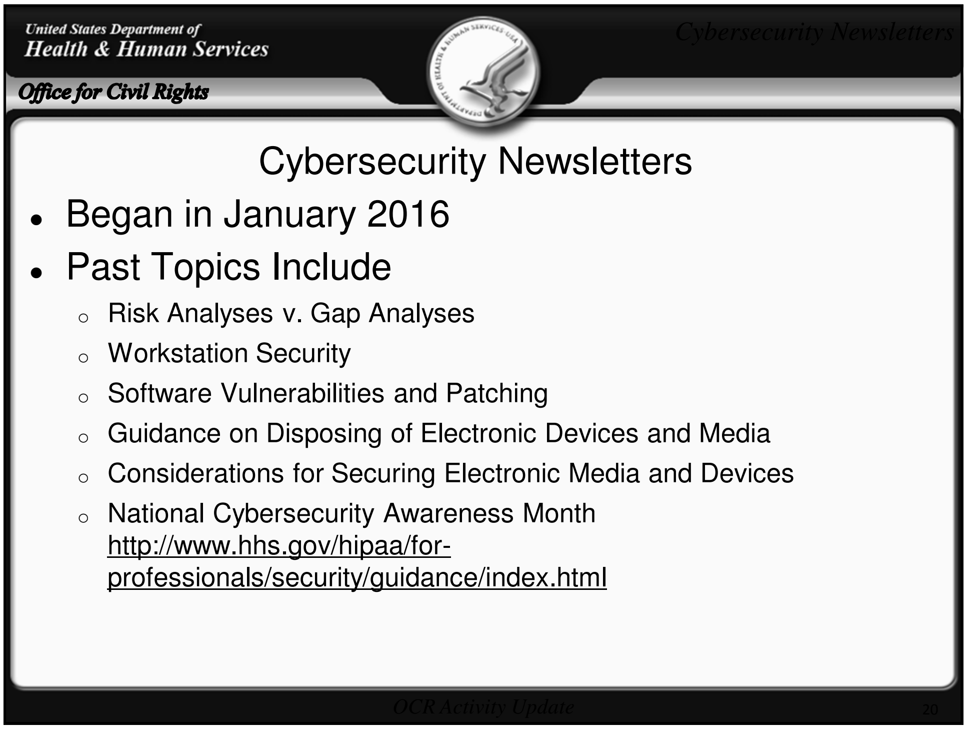
United States Department of
Health & Human Services
Office for Civil Rights

Cybersecurity Guidance page

Cyber Security Guidance Material

- HHS OCR has launched a Cyber Security Guidance Material webpage, including a Cyber Security Checklist and Infographic, which explain the steps for a HIPAA covered entity or its business associate to take in response to a cyber-related security incident.
  - Cyber Security Checklist - PDF
  - Cyber Security Infographic [GIF 802 KB]

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

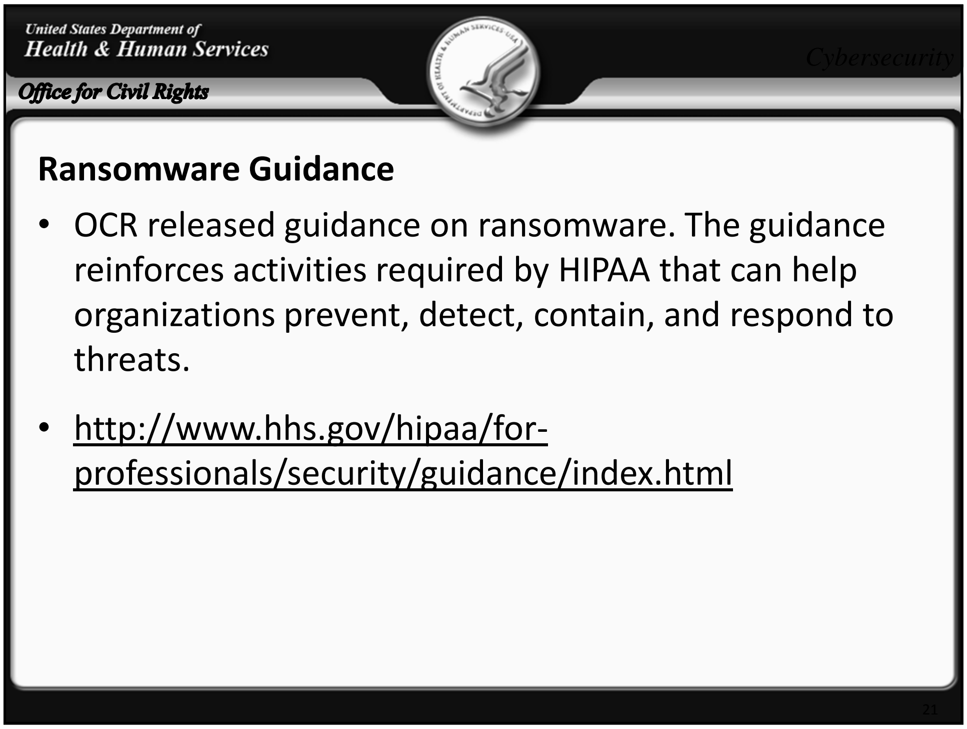


United States Department of
Health & Human Services
Office for Civil Rights

Cybersecurity Newsletters

Cybersecurity Newsletters

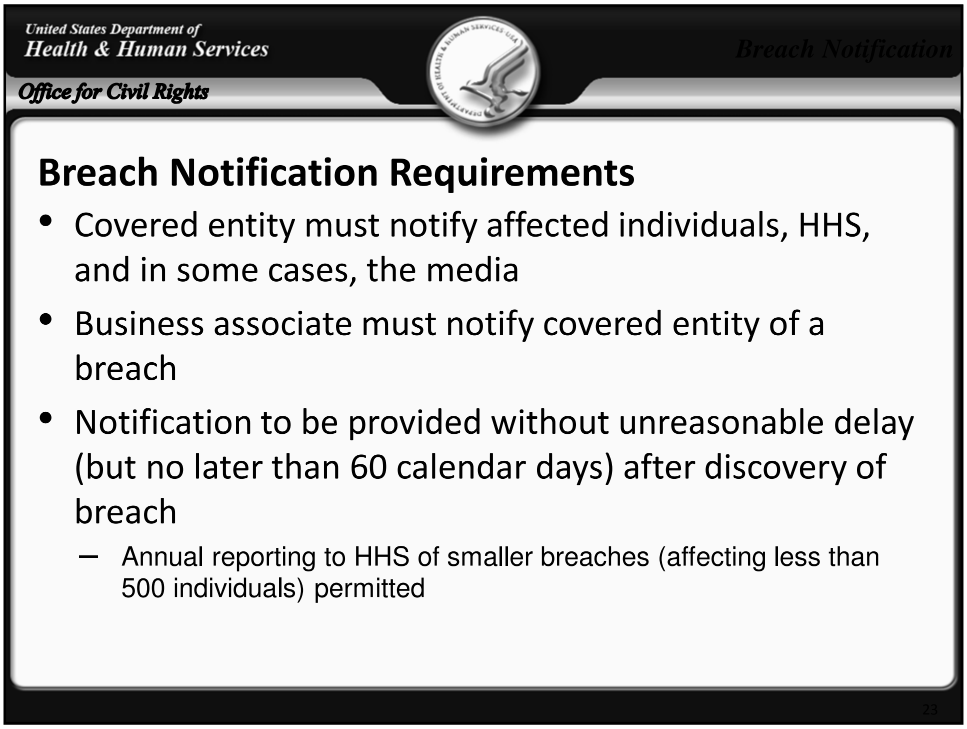
- Began in January 2016
- Past Topics Include
  - Risk Analyses v. Gap Analyses
  - Workstation Security
  - Software Vulnerabilities and Patching
  - Guidance on Disposing of Electronic Devices and Media
  - Considerations for Securing Electronic Media and Devices
  - National Cybersecurity Awareness Month http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html



Ransomware Guidance

- OCR released guidance on ransomware. The guidance reinforces activities required by HIPAA that can help organizations prevent, detect, contain, and respond to threats.
- http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY

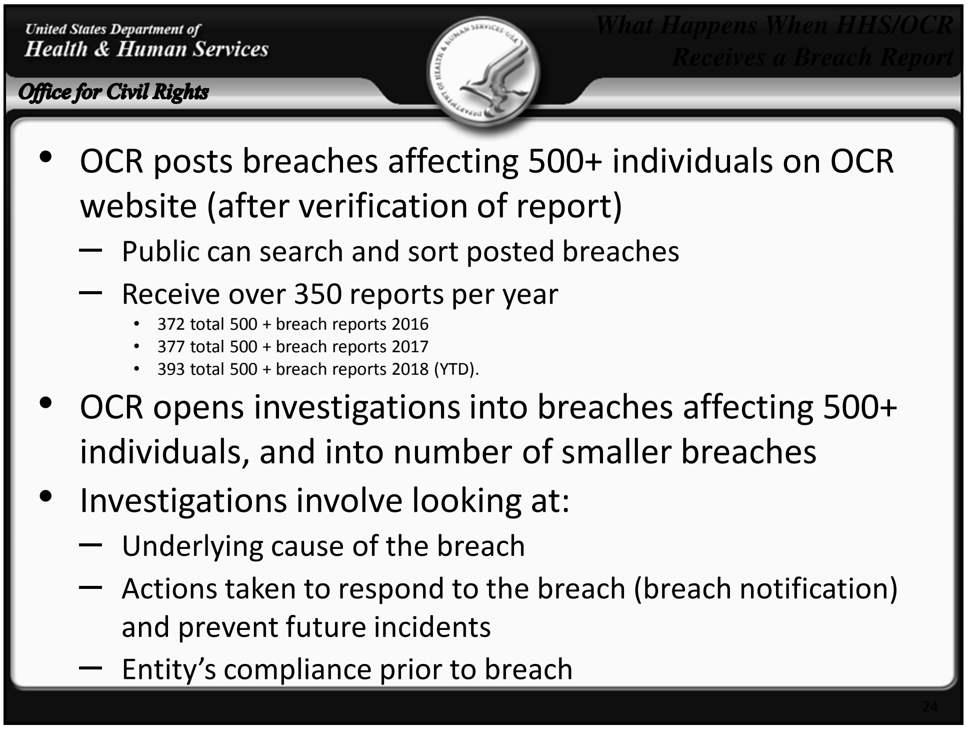


United States Department of
Health & Human Services
Office for Civil Rights

Breach Notification

Breach Notification Requirements

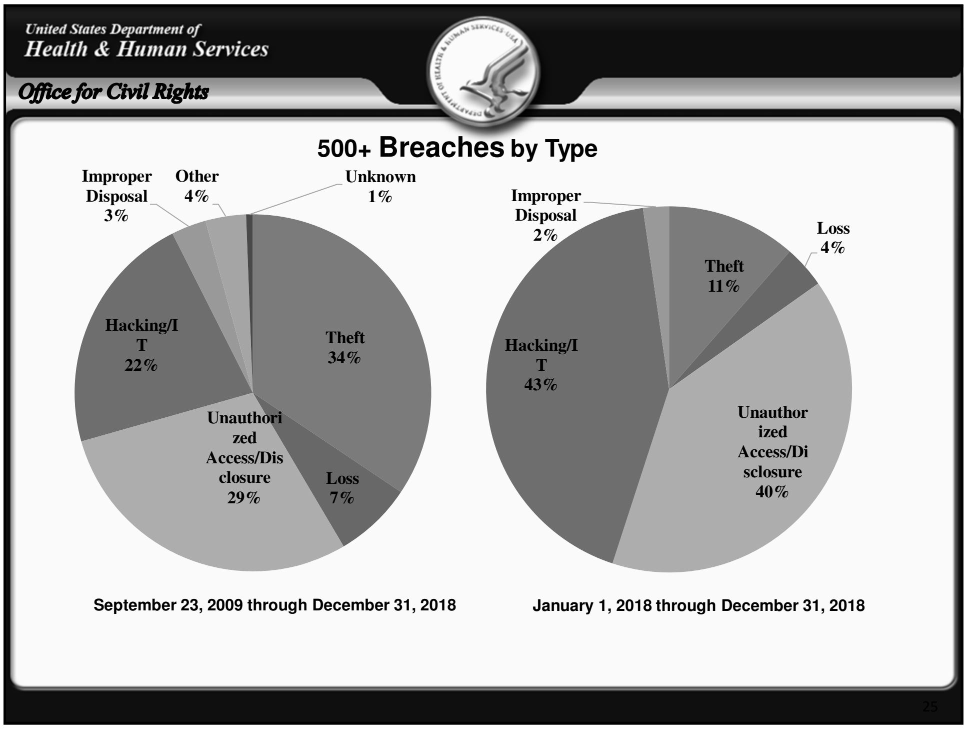
- Covered entity must notify affected individuals, HHS, and in some cases, the media
- Business associate must notify covered entity of a breach
- Notification to be provided without unreasonable delay (but no later than 60 calendar days) after discovery of breach
  - Annual reporting to HHS of smaller breaches (affecting less than 500 individuals) permitted



United States Department of
Health & Human Services
Office for Civil Rights

What Happens When HHS/OCR Receives a Breach Report

- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
  - Public can search and sort posted breaches
  - Receive over 350 reports per year
    - 372 total 500 + breach reports 2016
    - 377 total 500 + breach reports 2017
    - 393 total 500 + breach reports 2018 (YTD).
- OCR opens investigations into breaches affecting 500+ individuals, and into number of smaller breaches
- Investigations involve looking at:
  - Underlying cause of the breach
  - Actions taken to respond to the breach (breach notification) and prevent future incidents
  - Entity’s compliance prior to breach



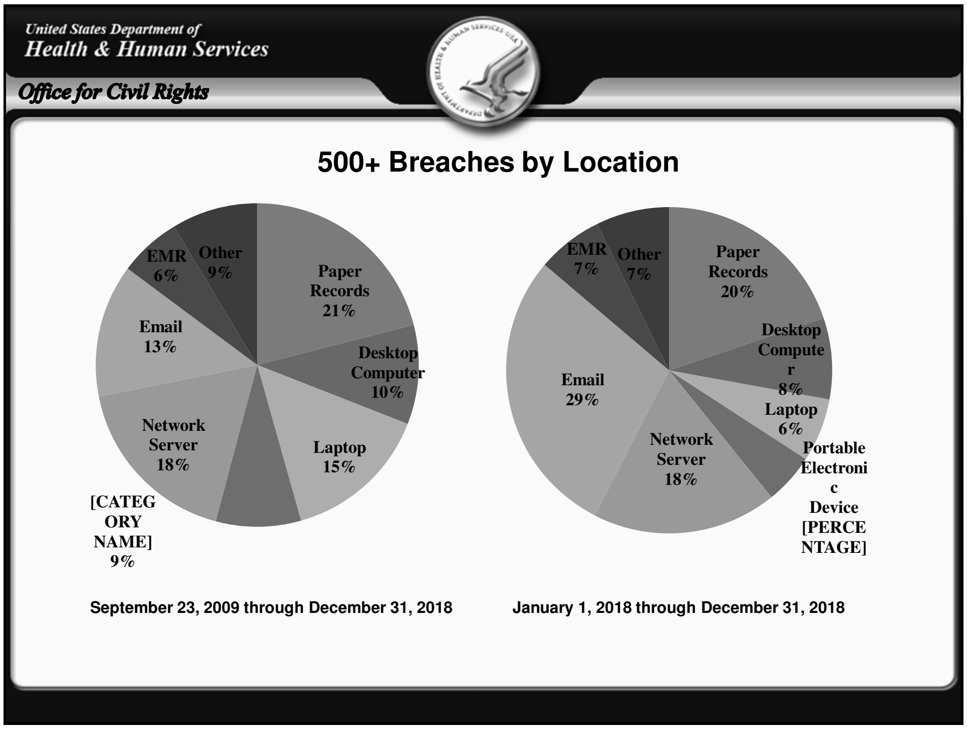
United States Department of
Health & Human Services

Office for Civil Rights

500+ Breaches by Type

September 23, 2009 through December 31, 2018

January 1, 2018 through December 31, 2018



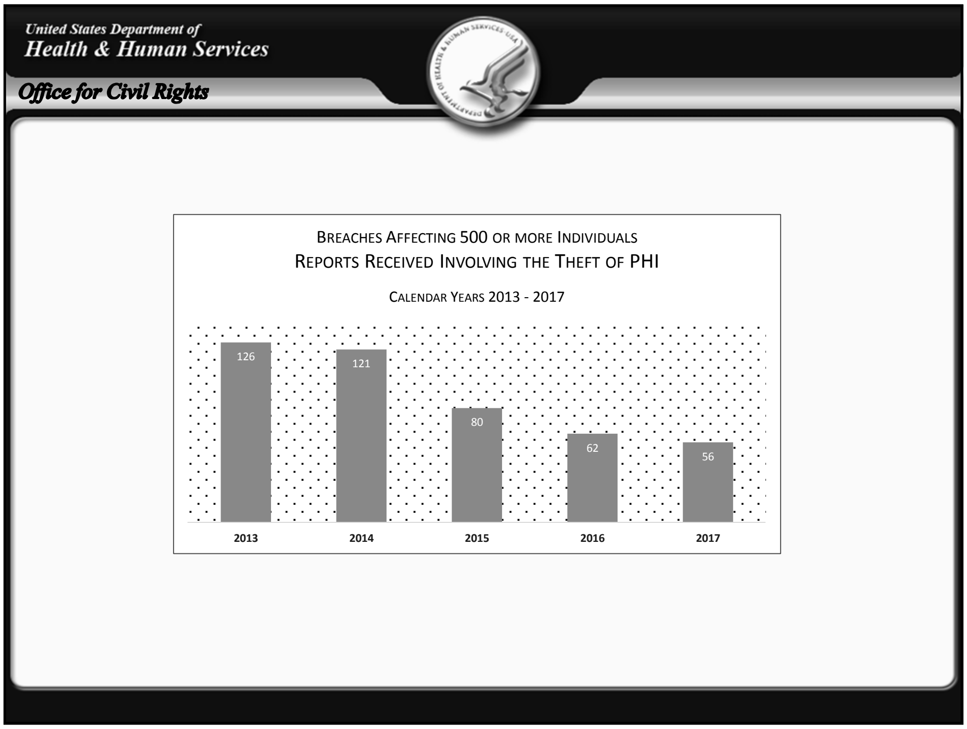
United States Department of
Health & Human Services

Office for Civil Rights

500+ Breaches by Location

September 23, 2009 through December 31, 2018

January 1, 2018 through December 31, 2018

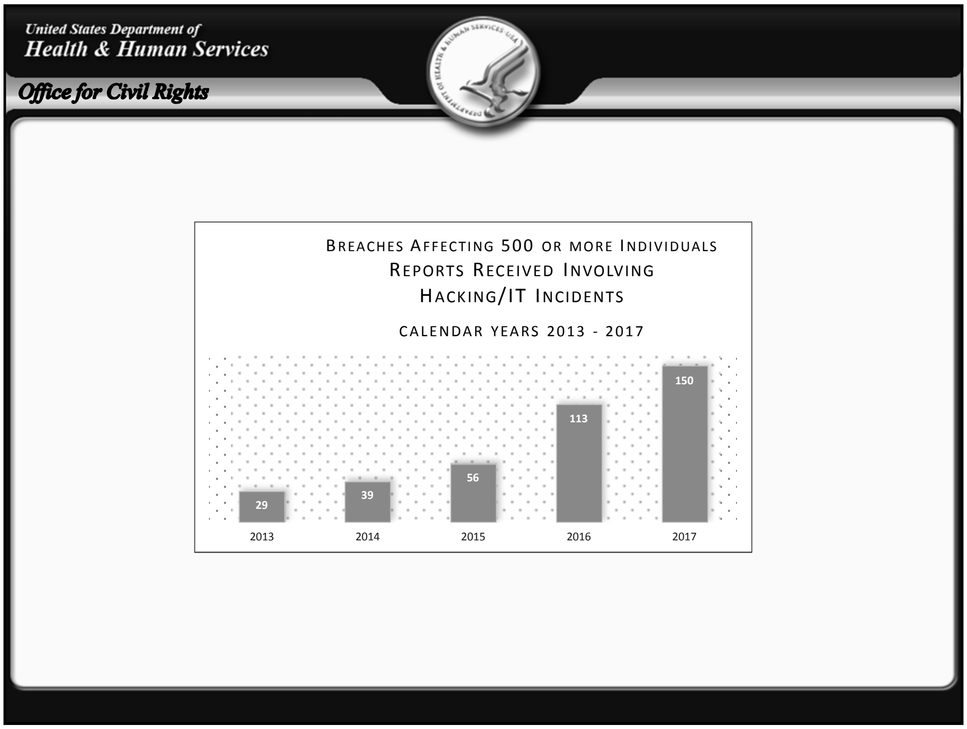


United States Department of
Health & Human Services

Office for Civil Rights

Breaches Affecting 500 or more Individuals
Reports Received Involving the Theft of PHI

Calendar Years 2013 - 2017

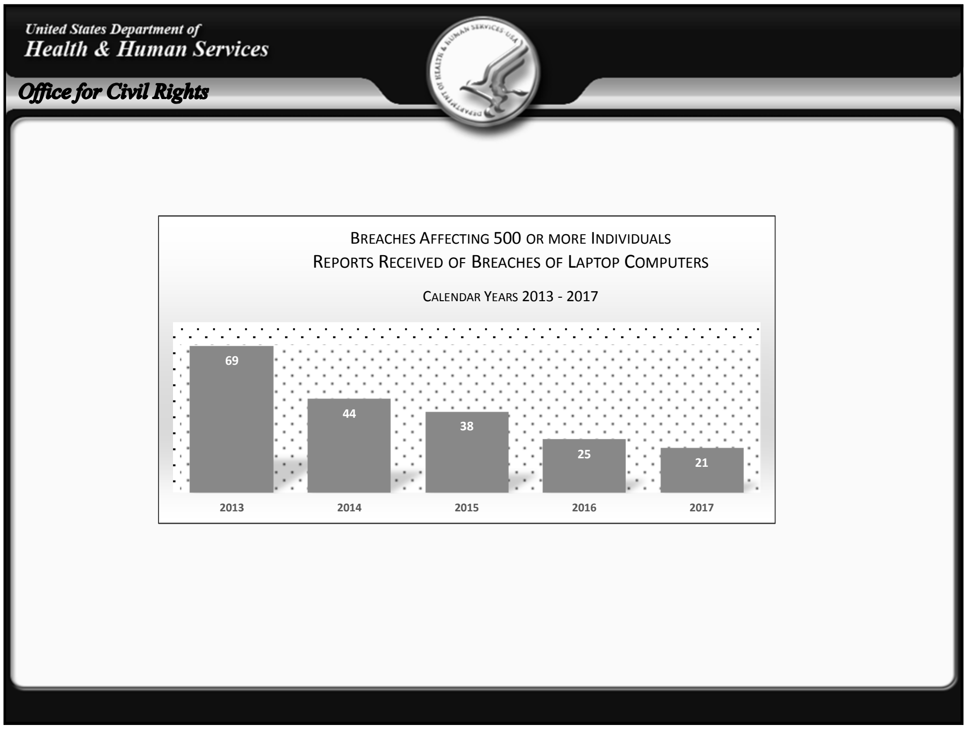


United States Department of
Health & Human Services

Office for Civil Rights

Breaches Affecting 500 or more Individuals
Reports Received Involving
Hacking/IT Incidents

Calendar Years 2013 - 2017

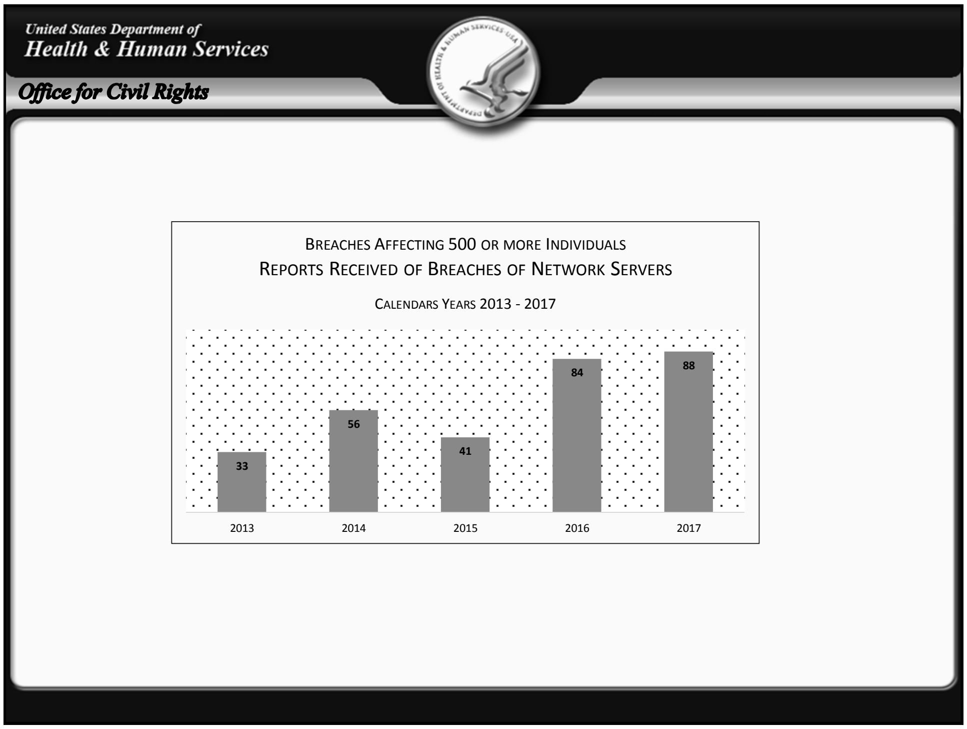


United States Department of
Health & Human Services

Office for Civil Rights

BREACHES AFFECTING 500 OR MORE INDIVIDUALS
REPORTS RECEIVED OF BREACHES OF LAPTOP COMPUTERS

CALENDAR YEARS 2013 - 2017

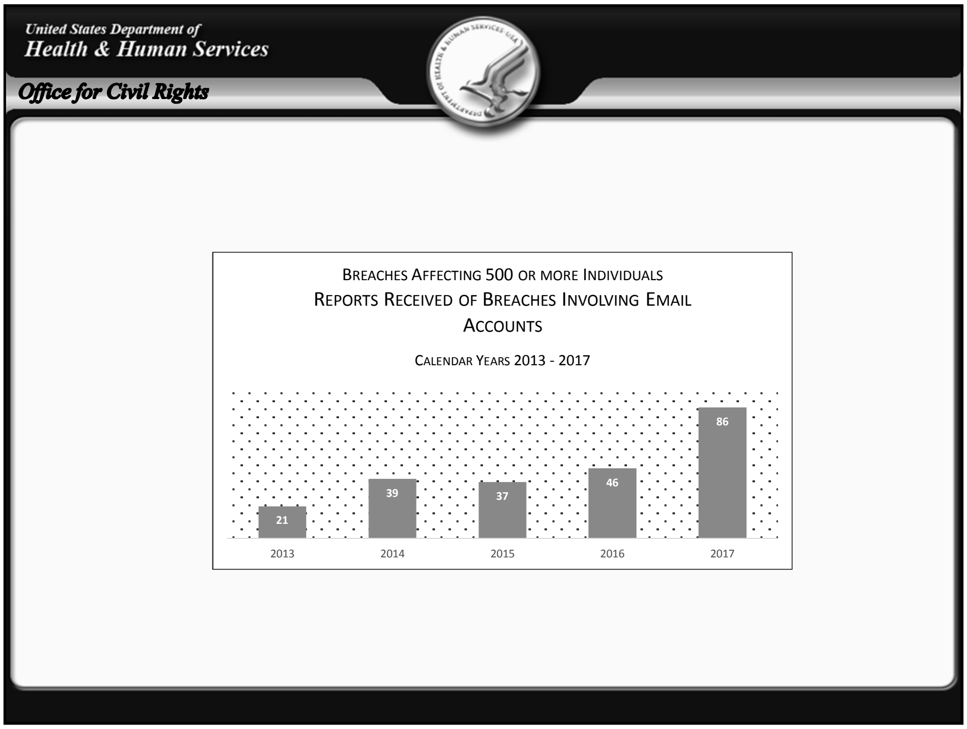


United States Department of
Health & Human Services

Office for Civil Rights

BREACHES AFFECTING 500 OR MORE INDIVIDUALS
REPORTS RECEIVED OF BREACHES OF NETWORK SERVERS

CALENDARS YEARS 2013 - 2017

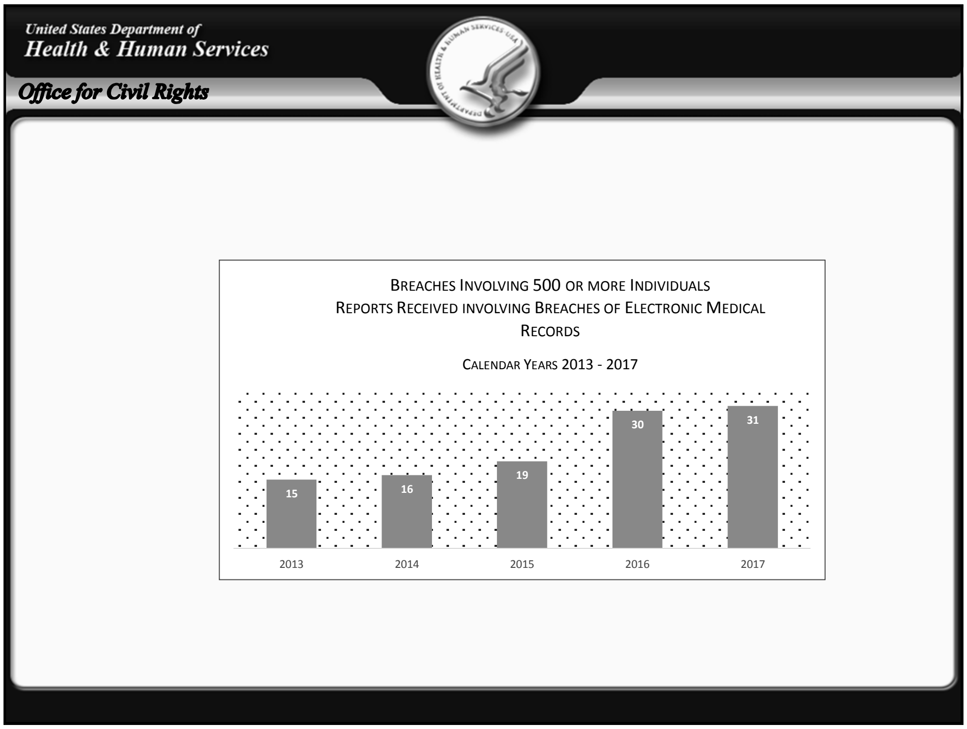


United States Department of
Health & Human Services

Office for Civil Rights

BREACHES AFFECTING 500 OR MORE INDIVIDUALS
REPORTS RECEIVED OF BREACHES INVOLVING EMAIL ACCOUNTS

CALENDAR YEARS 2013 - 2017

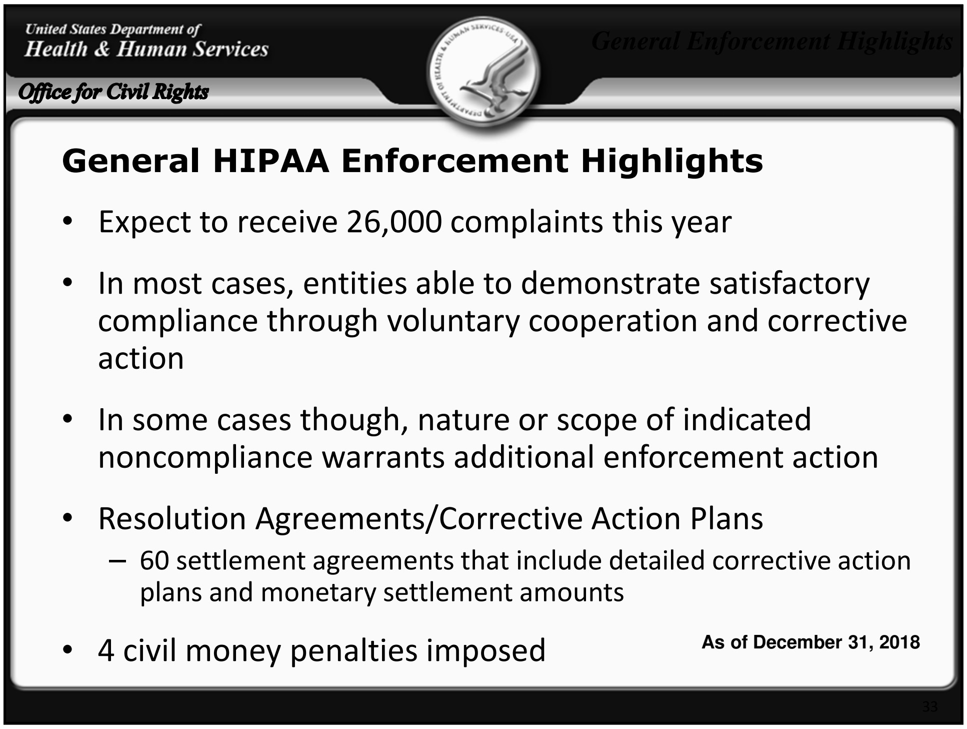


United States Department of
Health & Human Services

Office for Civil Rights

BREACHES INVOLVING 500 OR MORE INDIVIDUALS
REPORTS RECEIVED INVOLVING BREACHES OF ELECTRONIC MEDICAL RECORDS

CALENDAR YEARS 2013 - 2017



United States Department of
Health & Human Services
Office for Civil Rights

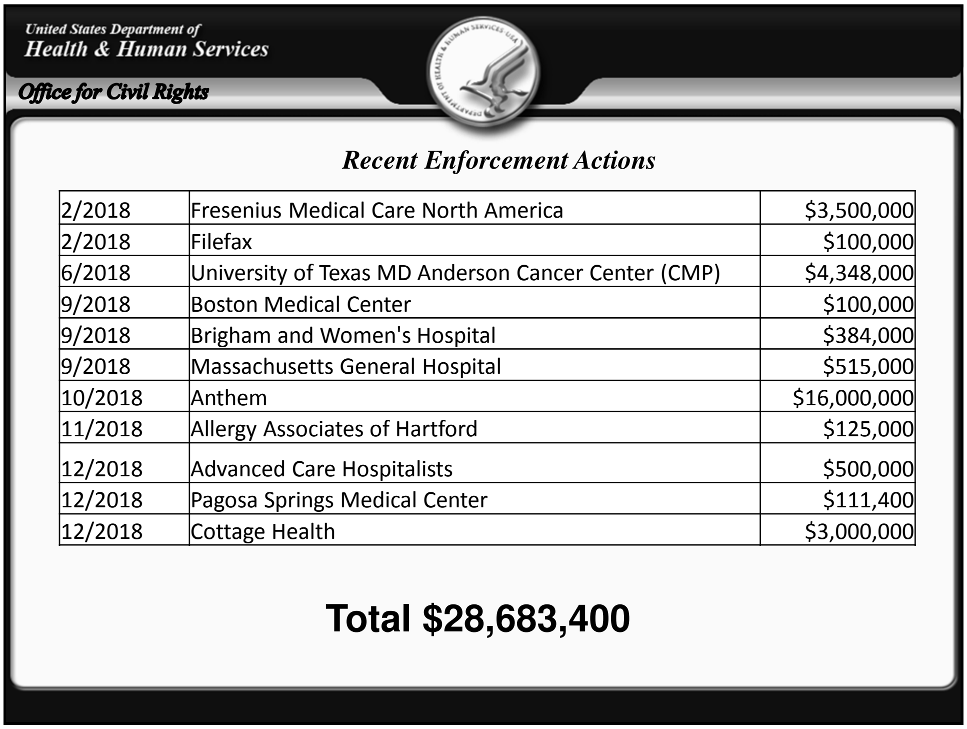
General Enforcement Highlights

General HIPAA Enforcement Highlights

- Expect to receive 26,000 complaints this year
- In most cases, entities able to demonstrate satisfactory compliance through voluntary cooperation and corrective action
- In some cases though, nature or scope of indicated noncompliance warrants additional enforcement action
- Resolution Agreements/Corrective Action Plans
  - 60 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 4 civil money penalties imposed

As of December 31, 2018

33

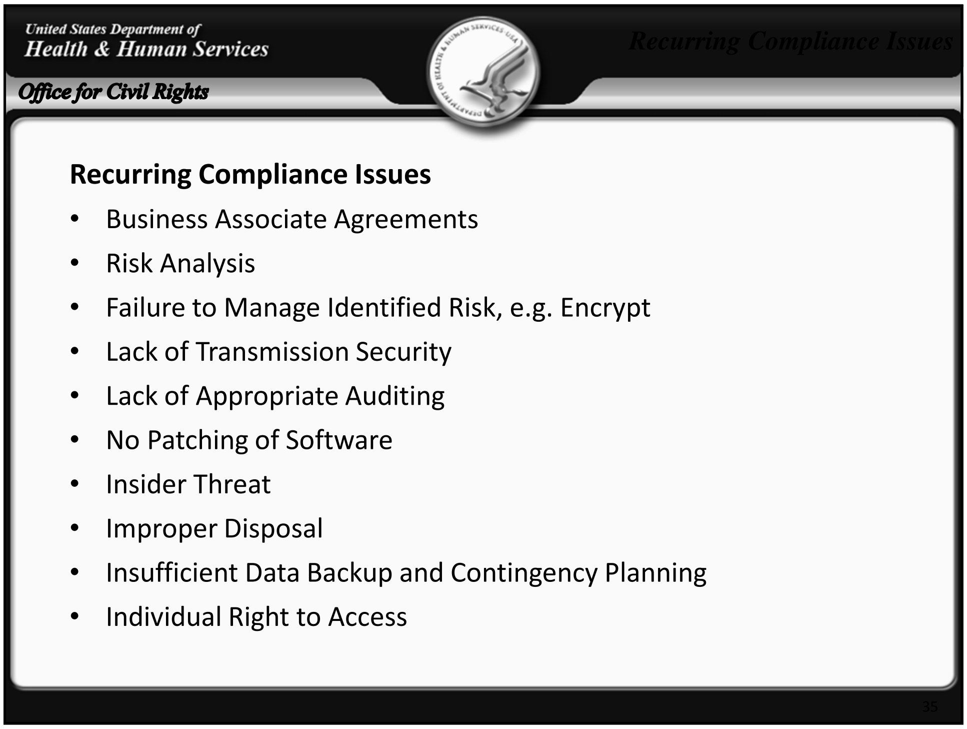


United States Department of
Health & Human Services
Office for Civil Rights

Recent Enforcement Actions

2/2018	Fresenius Medical Care North America	$3,500,000
2/2018	Filefax	$100,000
6/2018	University of Texas MD Anderson Cancer Center (CMP)	$4,348,000
9/2018	Boston Medical Center	$100,000
9/2018	Brigham and Women's Hospital	$384,000
9/2018	Massachusetts General Hospital	$515,000
10/2018	Anthem	$16,000,000
11/2018	Allergy Associates of Hartford	$125,000
12/2018	Advanced Care Hospitalists	$500,000
12/2018	Pagosa Springs Medical Center	$111,400
12/2018	Cottage Health	$3,000,000

Total $28,683,400



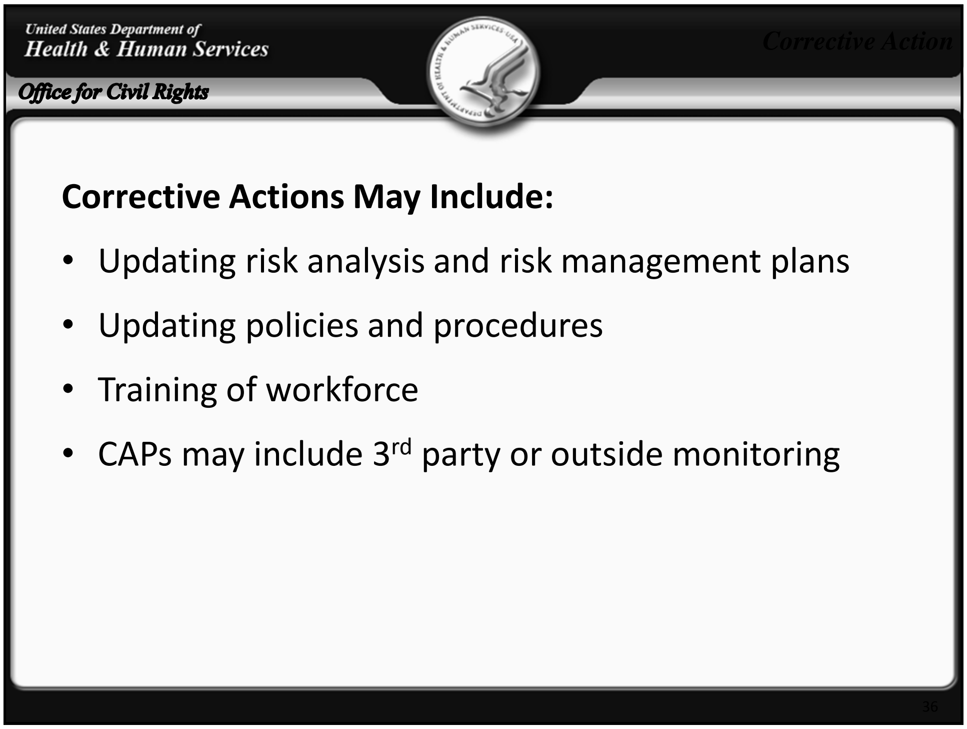
United States Department of
Health & Human Services

Office for Civil Rights

Recurring Compliance Issues

Recurring Compliance Issues

- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, e.g. Encrypt
- Lack of Transmission Security
- Lack of Appropriate Auditing
- No Patching of Software
- Insider Threat
- Improper Disposal
- Insufficient Data Backup and Contingency Planning
- Individual Right to Access



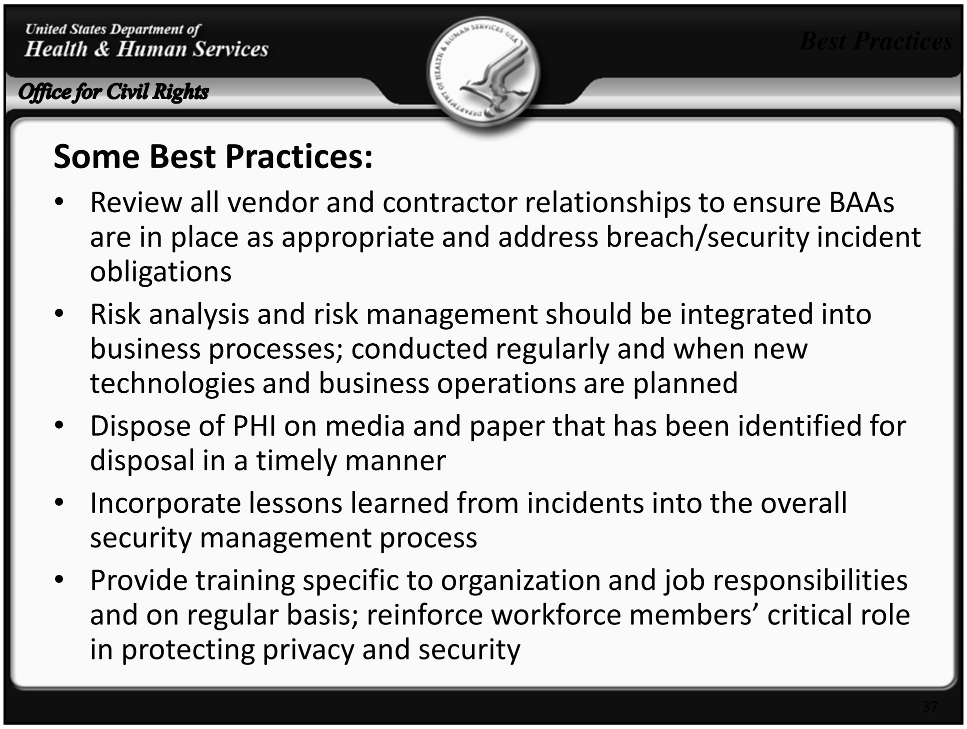
United States Department of
Health & Human Services

Office for Civil Rights

Corrective Action

Corrective Actions May Include:

- Updating risk analysis and risk management plans
- Updating policies and procedures
- Training of workforce
- CAPs may include 3rd party or outside monitoring



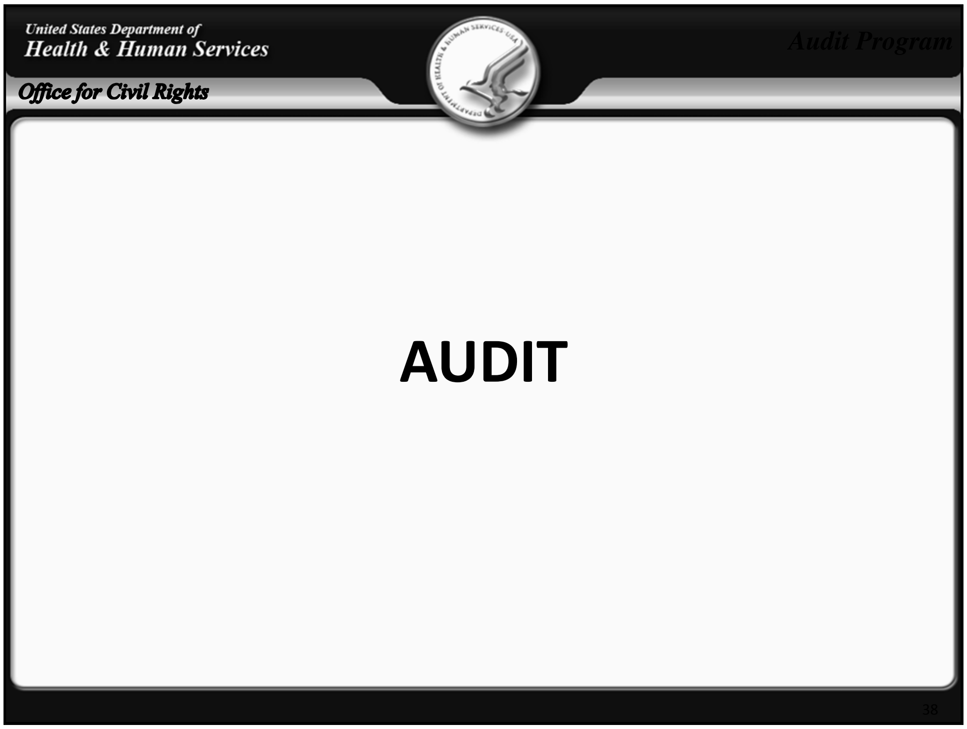
United States Department of
Health & Human Services

Office for Civil Rights

Best Practices

Some Best Practices:

- Review all vendor and contractor relationships to ensure BAAs are in place as appropriate and address breach/security incident obligations
- Risk analysis and risk management should be integrated into business processes; conducted regularly and when new technologies and business operations are planned
- Dispose of PHI on media and paper that has been identified for disposal in a timely manner
- Incorporate lessons learned from incidents into the overall security management process
- Provide training specific to organization and job responsibilities and on regular basis; reinforce workforce members' critical role in protecting privacy and security

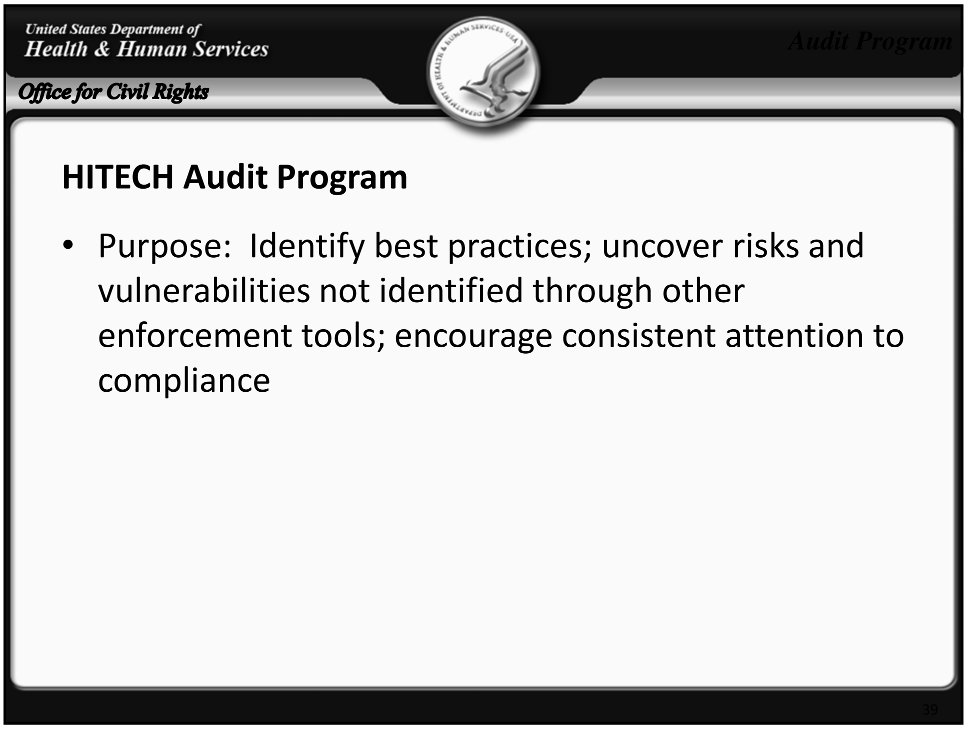


United States Department of
Health & Human Services

Office for Civil Rights

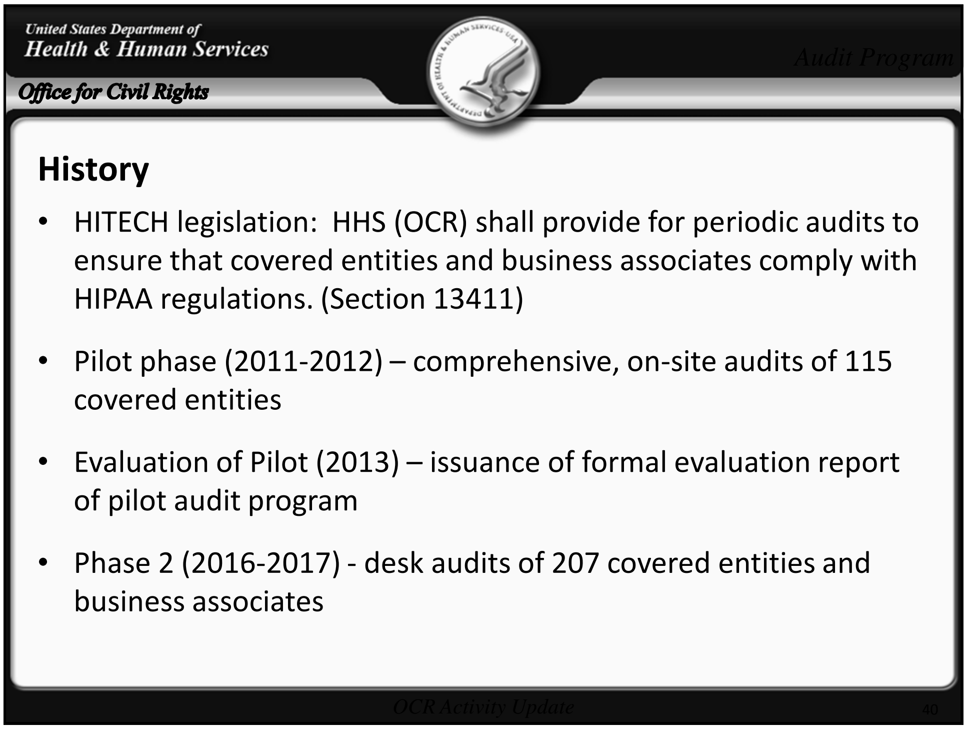
Audit Program

AUDIT



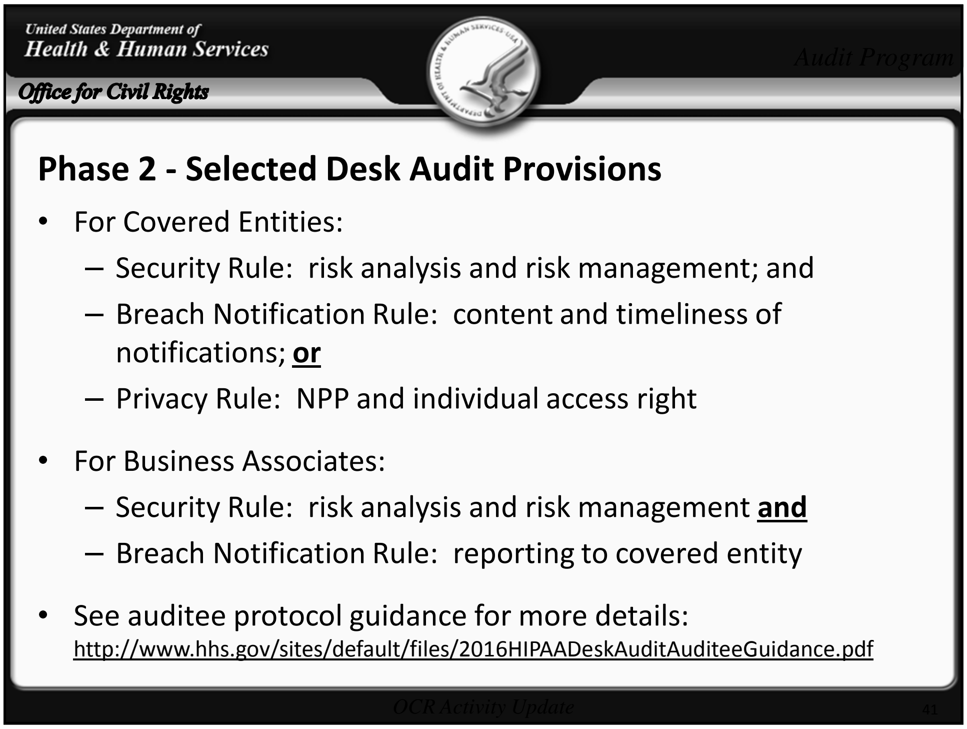
HITECH Audit Program

- Purpose: Identify best practices; uncover risks and vulnerabilities not identified through other enforcement tools; encourage consistent attention to compliance



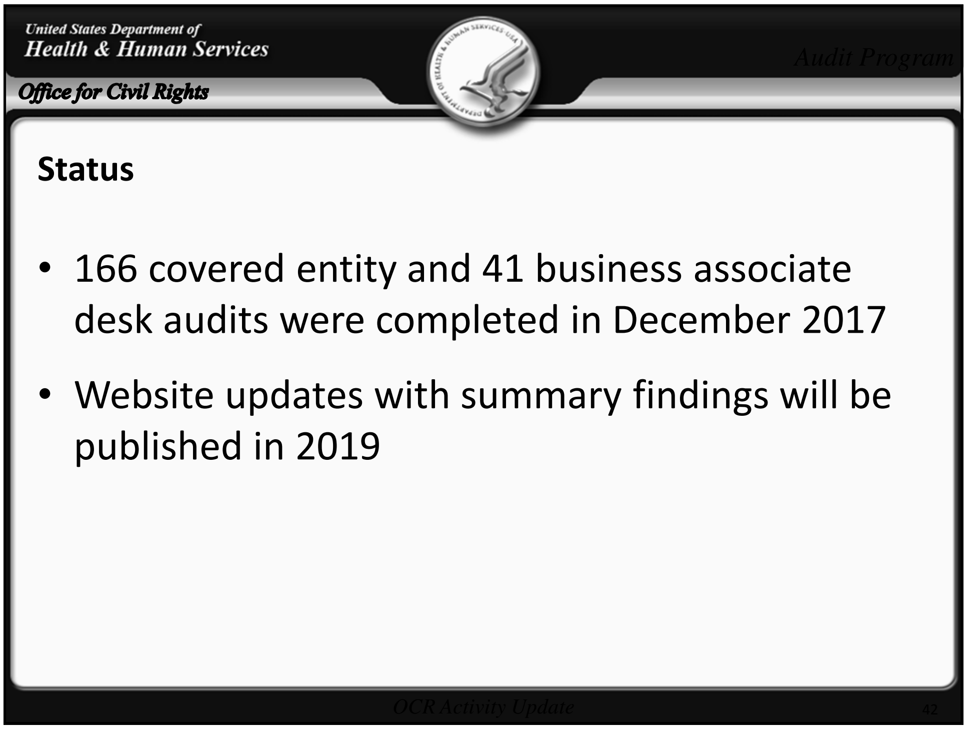
History

- HITECH legislation: HHS (OCR) shall provide for periodic audits to ensure that covered entities and business associates comply with HIPAA regulations. (Section 13411)
- Pilot phase (2011-2012) – comprehensive, on-site audits of 115 covered entities
- Evaluation of Pilot (2013) – issuance of formal evaluation report of pilot audit program
- Phase 2 (2016-2017) - desk audits of 207 covered entities and business associates



Phase 2 - Selected Desk Audit Provisions

- For Covered Entities:
  - Security Rule: risk analysis and risk management; and
  - Breach Notification Rule: content and timeliness of notifications; **or**
  - Privacy Rule: NPP and individual access right
- For Business Associates:
  - Security Rule: risk analysis and risk management **and**
  - Breach Notification Rule: reporting to covered entity
- See auditee protocol guidance for more details: http://www.hhs.gov/sites/default/files/2016HIPAADeskAuditAuditeeGuidance.pdf



Status

- 166 covered entity and 41 business associate desk audits were completed in December 2017
- Website updates with summary findings will be published in 2019

Provider Education: An Individual's Right to Access and Obtain their Health Information Under HIPAA

- **Web-based Video Training for Free Continuing Medical Education and Continuing Education Credit for Health Care Professionals via Medscape**

http://www.medscape.org/viewarticle/876110

Right to Access Your Health Information Under HIPAA

Phase 2 of OCR's *Information is Powerful Medicine* Campaign

Information is key to making good health care decisions. Understand your health history to ask better questions and make healthier choices. Track your lab results and medications, get x-rays and other medical images, or share your information with a caregiver or a research program.

Clear and concise
Get it: Covers Form and Format and Manner of Access, Time and Timeliness, Fees
Check it: Check to make sure your health information is correct and complete
Use it: Right to Third Party Access, including a researcher.

Includes:
Links to Fact Sheets and FAQs, Videos, Poster, Brochure
Digital Ads and Banners, Mobile Platform
Also – a link to join All of Us Research Initiative

INFORMATION IS POWERFUL MEDICINE
Access to your health information is your right
Get it. Check it. Use it.

HHS.gov/GetItCheckItUseIt

United States Department of
Health & Human Services

Office for Civil Rights

More Information

http://www.hhs.gov/hipaa

Join us on Twitter @hhsocr