

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



## Update on Administration and Enforcement of the HIPAA Privacy, Security, and Breach Notification Rules

Valerie Montoya, Investigator  
Office for Civil Rights (OCR)  
U.S. Department of Health and Human Services

April 27, 2018

---

---

---

---

---

---

---

---

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



### Updates

- Policy Development
- Breach Notification
- Enforcement
- Audit

---

---

---

---

---

---

---

---

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



## POLICY DEVELOPMENT

---

---

---

---

---

---

---

---

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



### New 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:
  - New tab for mental health in “FAQs for Professionals”
  - 9 new FAQs added (as PDF and in database)
- New Materials for Professionals and Consumers
  - Fact Sheets for Specific Audiences
  - Information-sharing Decision Charts

---

---

---

---

---

---

---

---

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



### OCR Website Navigation

- 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>

---

---

---

---

---

---

---

---

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



### 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

---

---

---

---

---

---

---

---

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



Access Guidelines

### 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)

---

---

---

---

---

---

---

---

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



Access Guidelines

### 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

---

---

---

---

---

---

---

---

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



Access Guidelines

### 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

---

---

---

---

---

---

---

---

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



Access Guidelines

### 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

---

---

---

---

---

---

---

---

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



Access Guidelines

### 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
  - Must inform individual in advance of approximate fee

---

---

---

---

---

---

---

---

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



Access Guidelines

### 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)

---

---

---

---

---

---

---

---

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

Platform for users to influence guidance  
Health Information Privacy, Security and Breach Notification Rules

### 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

---

---

---

---

---

---

---

---

---

---

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

Platform for users to influence guidance  
Health Information Privacy, Security and Breach Notification Rules

Health app developers, what are your questions about HIPAA?

Welcome Learn More Questions Helpful Links Contact

HIPAA Health Information Privacy, Security and Breach Notification Rules  
About HIPAA

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

October 2015

---

---

---

---

---

---

---

---

---

---

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

Platform for users to influence guidance  
Health Information Privacy, Security and Breach Notification Rules

### 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/2014/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



### 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

- Began in January 2016
- Recent 2017-2018 Newsletters
  - October 2017 (Mobile Devices and PHI)
  - November 2017 (Insider Threats and Termination Procedures)
  - December 2017 (Cybersecurity While on Holiday)
  - January 2018 (Cyber Extortion)
  - February 2018 (Phishing)
- <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>

---

---

---

---

---

---

---

---

---

---

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



### Ransomware Guidance

- OCR recently released guidance on ransomware. The new 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>

---

---

---

---

---

---

---

---

---

---

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



## BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY

---

---

---

---

---

---

---

---

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



### Breach Notification Requirements

- Covered entity must notify affected individuals, HHS, and in some cases, the media, of breach
- Business associate must notify covered entity of 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
- OCR posts breaches affecting 500+ individuals on OCR website

---

---

---

---

---

---

---

---

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



### HIPAA Breach Highlights

#### September 2009 through February 28, 2018

- Approximately 2,222 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 46% of large breaches
  - Hacking/IT now account for 19% of incidents
  - Laptops and other portable storage devices account for 25% of large breaches
  - Paper records are 21% of large breaches
  - Individuals affected are approximately 177,298,024
- Approximately 341,002 reports of breaches of PHI affecting fewer than 500 individuals

---

---

---

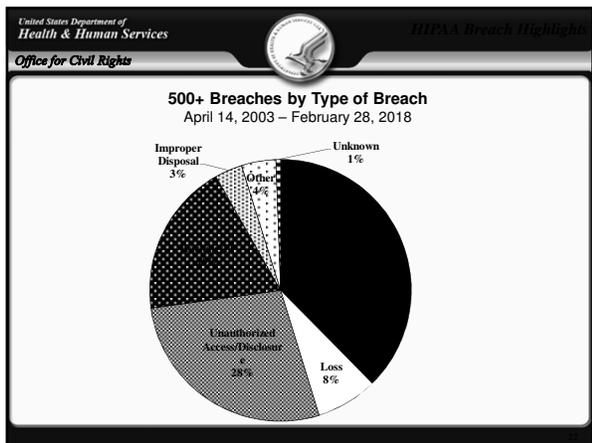
---

---

---

---

---



---

---

---

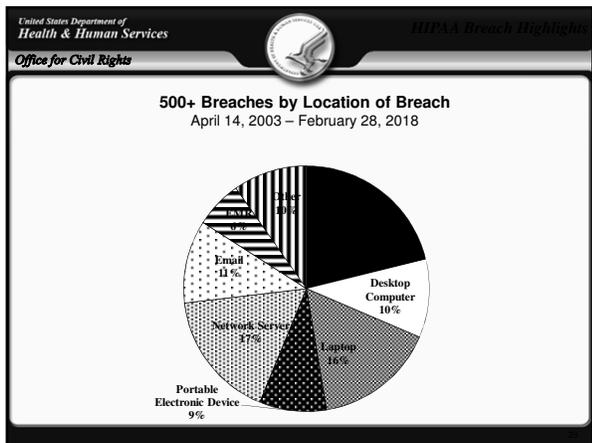
---

---

---

---

---



---

---

---

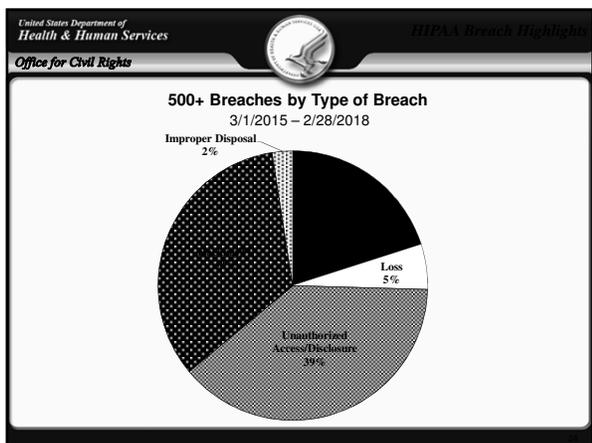
---

---

---

---

---



---

---

---

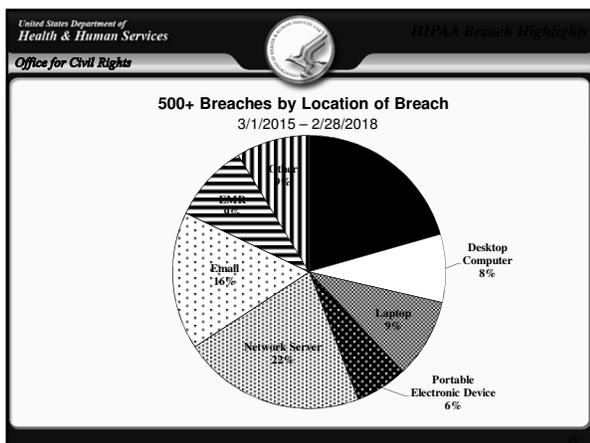
---

---

---

---

---



---

---

---

---

---

---

---

---

- United States Department of Health & Human Services  
Office for Civil Rights  
HIPAA Breach Highlights
- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
    - Public can search and sort posted breaches
  - 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 (including compliance with breach notification requirements) and prevent future incidents
    - Entity's compliance prior to breach

---

---

---

---

---

---

---

---

- United States Department of Health & Human Services  
Office for Civil Rights  
General Enforcement Highlights
- ### General HIPAA Enforcement Highlights as of April 14, 2003 – February, 2018
- Over 175,534 complaints received to date
  - Over 25,742 cases resolved with corrective action and/or technical assistance
  - Expect to receive 24,000 complaints this year

---

---

---

---

---

---

---

---

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

- 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
  - 52 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 3 civil money penalties

As of February 28, 2018

---

---

---

---

---

---

---

---

---

---

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

2017 - 2018

4/12/2017	Metro Community Provider Network	\$400,000
4/21/2017	Center for Children's Digestive Health	\$31,000
4/21/2017	CardioNet	\$2,500,000
5/10/2017	Memorial Hermann Health System	\$2,400,000
5/23/2017	St. Luke's-Roosevelt Hospital Center	\$387,200
12/28/2017	21st Century Oncology	\$2,300,000
2/1/2018	Fresenius Medical Care North America	\$3,500,000
2/13/2018	Filefax	\$100,000
<b>Total</b>		<b>\$11,618,200</b>

---

---

---

---

---

---

---

---

---

---

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

---

---

---

---

---

---

---

---

---

---

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

**Corrective Actions**

**Corrective Actions May Include:**

- Updating risk analysis and risk management plans
- Updating policies and procedures
- Training of workforce
- Implementing specific technical or other safeguards
- Mitigation
- CAPs may include 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 Programs**

**AUDIT**

---

---

---

---

---

---

---

---

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



**HITECH Audit Program**

- Purpose: Identify best practices; uncover risks and vulnerabilities not identified through other enforcement tools; encourage consistent attention to compliance
  - Intended to be non-punitive, but OCR can open a compliance review (for example, if significant concerns are raised during an audit)
  - Learn from Phase 2 in structuring permanent audit program

---

---

---

---

---

---

---

---

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



**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

---

---

---

---

---

---

---

---

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



**Phase 2 - Selected Desk Audit Provisions**

- For Covered Entities:
  - Security Rule: risk analysis and risk management;
  - 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>

---

---

---

---

---

---

---

---

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

**Status**

- 166 covered entity and 41 business associate desk audits were completed in December 2017
- After Phase 2, more comprehensive on-site audits will be conducted as a part of the permanent audit program
  - On-site audits will evaluate auditees against a comprehensive selection of controls in the audit protocol:  
<http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/>
- Website updates with summary findings will be published summer 2018

---

---

---

---

---

---

---

---

---

---

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

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

---

---

---

---

---

---

---

---

---

---

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

**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>

---

---

---

---

---

---

---

---

---

---

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



**Consumer Facing Resources:**  
**Right to Access Your Health Information Under HIPAA**

---

---

---

---

---

---

---

---

---

---

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

New Consumer Facing Tools

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

Learn about HIPAA and your health information rights at: [www.HHS.gov/OCR/CheckItUseIt](http://www.HHS.gov/OCR/CheckItUseIt)

---

---

---

---

---

---

---

---

---

---

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

Pocket Brochure, Exterior and Interior Flap

**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.

**POCKET BROCHURE**

Know your rights. Take control. Get better care.

---

---

---

---

---

---

---

---

---

---

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

**Pocket Brochure Interior View**

Health records are a powerful tool in managing your care

**GET IT**

You have the right to see and get copies of your health information. To help make sure you get a copy of the info you want, it's best to be ready when your doctor normally has up to 30 days to provide you a copy of your information, your doctor often can provide the information much sooner than that. If your doctor often is not seeing you, they are able to easily view and download your health information whenever you want.



**CHECK IT**

There are a few exceptions to getting your information. You can't be denied access for not paying your medical bill. Your doctor, OH, however, change you a reasonable fee for a copy of your health information. The fee may not be as large as if your information is stored electronically.



**USE IT**

Having access to your health information makes better communication between you and your doctor. You can understand your health. You can control your health. You can share your information directly with others. You can participate in your or a family member's care.

**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.

---

---

---

---

---

---

---

---

---

---

---

---

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

**HHS.gov/GetItCheckItUseIt**



**Clear and concise**

- Links to Fact Sheets and FAQs
- Videos
- Poster
- Brochure
- Digital Ads and Banners
- Mobile Platform
- Link to Join All of Us Research Initiative

---

---

---

---

---

---

---

---

---

---

---

---

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

**More Information**

<http://www.hhs.gov/hipaa>

Join us on Twitter @hhsocr

---

---

---

---

---

---

---

---

---

---

---

---

United States Department of  
*Health & Human Services*



Office for Civil Rights

**Questions?**

Valerie Montoya, Investigator  
214-767-1717 Direct  
Valerie.Montoya@hhs.gov

---

---

---

---

---

---

---

---