HIPAA Update

Linda Sanches, Senior Advisor, Health IT & Privacy Policy
HHS Office for Civil Rights

HCCA Compliance Institute  April 8, 2019

What is OCR?

- Part of the Office of the Secretary, Department of Health and Human Services.
- Headquartered in D.C. with 8 regional offices (in 11 locations) across the U.S.
- 3 Divisions – Civil Rights, Conscience and Religious Freedom and Health Information Privacy
- HIP enforces the HIPAA Privacy, Security, and Breach Notification Rules through
  • regulations and technical assistance, as well as
  • outreach to the regulated community and
  • to the public to increase individuals’ awareness of their HIPAA rights and protections.
Agenda

- Breach Notification Highlights
- Recent Enforcement Actions
- 2019 Enforcement Initiatives
- Current Policy Initiatives

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

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
Breach Reporting – What Should be Reported?

- Acquisition, access, use, or disclosure of PHI in a manner not permitted under Privacy Rule which compromises the security or privacy of the PHI.
- 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
- Breach risk assessment must be documented

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 affecting 500+ individuals per year
- 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
Breaches Reported Involving the Theft of PHI

* Breaches Affecting 500 or more Individuals

Breaches Reported Involving Hacking/IT Incidents

* Breaches Affecting 500 or more Individuals
500+ Breaches by Type

September 23, 2009 through December 31, 2018

- Theft: 34%
- Unauthorized Access/Disclosure: 29%
- Hacking/IT: 22%
- Improper Disposal: 3%
- Loss: 7%
- Other: 4%
- Unknown: 1%

January 1, 2018 through December 31, 2018

- Theft: 11%
- Unauthorized Access/Disclosure: 43%
- Hacking/IT: 22%
- Improper Disposal: 2%
- Loss: 4%
- Other: 4%
- Unknown: 1%

Breaches Reported Involving Stolen Laptops

- 2014: 44 Breaches
- 2015: 38 Breaches
- 2016: 25 Breaches
- 2017: 21 Breaches
- 2018: 19 Breaches

* Breaches Affecting 500 or more Individuals
Recent Enforcement Actions

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

Total $28,683,400

2018 Enforcement Actions & Settlements

- **Fresenius Medical Care North America** – Multiple breaches lead to findings of failure to conduct adequate risk analysis and risk management -- $3,500,000
- **Filefax** – PHI liability for mishandling of PHI survives closure of business -- $100,000
2018 Enforcement Actions & Settlements

• **MD Anderson** – ALJ rules in favor of OCR following thefts of unencrypted media affecting over 33,500 individuals-- $4,348,000

• **ABC Cases (3)** – PHI disclosed during filming of Boston Med-- $999,000

• **Anthem** – Largest U.S. PHI breach in history. OCR investigation find inadequate safeguards to prevent and address spearphishing attacks- $16,000,000.00

---

2018 Enforcement Actions & Settlements

• **Pagosa Springs Medical Center** – Hospital failed to terminate former employee remote access leading to impermissible disclosure – $111,400

• **Advanced Care Hospital PL** – Physicians group shares PHI with unknown vendor without a BAA – $500,000

• **Allergy Associates of Hartford, PC** – Doctor discloses PHI to reporter in response to dispute with patient – $125,000
2019 HIPAA Enforcement Initiatives

• Compliance reviews on the right of access
• Consideration of entities that do not report breaches

Current HIPAA Policy Initiatives

• Request for Information (RFI) on Modifying HIPAA Rules To Improve Coordinated Care
  • Care coordination and case management
    • Right of Access
  • Opioid crisis and parental involvement in care
  • Notice of Privacy Practices
  • Accounting of Disclosures
• Comment Period closed Feb 12, 2019
• Public comments are now viewable at https://www.regulations.gov/docket?D=HHS-OCR-2018-0028
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

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
Access, HIPAA & Electronic Health Information (eHI) Exchange

New laws work with existing HIPAA rights to simplify how health care providers can meet individual requests for access to electronic health information.

The 2000 HIPAA Privacy Rule established an individual's right to access, inspect, and obtain a copy of health records, upon request, from a covered health care provider.

The 2009 HITECH Act directs HHS to adopt certification standards for electronic health record systems (EHRs), including methods for access, and to create rules for providers to use EHRs to provide individual access under Medicare enhanced payment programs.

The 2016 Cures Act directs HHS to develop the Trusted Exchange Framework and Common Agreement (TEFCA) for eHI exchange through health information networks (HINs) (Sec 4003) & to educate stakeholders about how eHI exchange can support individual access (Sec 4006).

Background: HIPAA Access

An individual has the right to request & receive a copy of medical, payment, and other records—Protected Health Information (PHI)—that providers and health plans use to make decisions about individuals:

- Doesn’t matter how old the PHI is, where it is kept, or where it originated
- Includes clinical lab test reports and underlying information

www.HHS.gov/HIPAA

An individual has the right to receive the information electronically & in her preferred form and format if the entity has the ability to readily produce it

45 CFR 164.524
### Current Federal Rules Automating Patient Access

**Under HIPAA**

Patients have **rights to an electronic copy** of their electronic PHI (ePHI) (including medical records) and **to have the provider electronically transmit PHI to another person** (45 CFR 164.524(c)).

Some records the individual requests may not be stored in the main EHR—providers may need to pull PHI from other digital systems or paper records to meet the request (45 CFR 164.524(a)(1); 164.501).

### HITECH MU Stage 3 Requirements

- View online, download & transmit their eHI, and/or
- Access their choice of 3rd party health apps using APIs

### ONC’s Developer Requirements for Certified EHRs (CEHRT Rule)

- Must implement API functions so app can retrieve whole or partial patient record
- Apply API security measures

---

### Health Records Can be Transmitted...

**Entities should find a method that satisfies the individual**

Support patients so they can use a secure electronic method to access their information:

- Through digital health apps that use open APIs
- Through view/download/transmit options (e.g. Blue Button)
- By secure email (or insecure, if requested by the individual) and direct messaging, through HINs, etc.
- Through patient portals
- Engage patients through online appointment scheduling, secure messaging, and prescription refills (see playbook)

Work with your vendors and/or HIN to enable these functions

---

[Image of network diagram]
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 & Exchange Assistance For Providers

• HIPAA Access Right Guidance and FAQs
• Guide to Privacy and Security
• Improving the Health Records Request Process for Patients
• Provider Access CME and CE
• Developer Portal
• OCR and ONC YouTube pages
• Patient Portals Guidance in the Patient Engagement Playbook
• Provider Playbook API Information & API education video
• Draft TEFCA
• Model Notice of Privacy Practices
Health IT Exchange Resources Related to Access

- **2015 Certification Requirements**
- **Developer Portal for HIT, business associate aid & more**
- **Health app scenarios guidance**
- **Best Practices for Electronic Health Information Exchange as required by Section 4006 of the Cures act are contained in the Draft TEFCA**
- **Draft USCDI**
- **Key Privacy & Security for APIs**

Access Information for Individuals

- **Your Rights Under HIPAA and HealthIT.gov/Access for Access videos & factsheets**
- **OCR and ONC YouTube pages**
- **Information is Powerful Medicine**
- **Trusted Exchange Highlights for Patients**
Consumer Outreach on Right of Access

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.

http://www.hhs.gov/getitcheckituseit

HHS.gov/GetItCheckItUseIt

Get it: Form, format & manner of access, timeliness, fees
Check it: Make sure your health information is correct and complete
Use it: Share with others including researchers & family caregivers
Free Continuing Medical Education and Continuing Education Credit for Health Care Professionals via Medscape


OCR Developer Portal

http://hipaaqsportal.hhs.gov/
Compliance Best Practices

• What are the elements of an effective risk analysis and risk management plan?
  • OCR Guidance
  • ONC Risk Assessment Tool

Web-based Video Training for Free
Continuing Medical Education via Medscape

56,000+ Trained on Right of Access from July 2017 – December 2018

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

Questions

• Visit us at http://www.hhs.gov/HIPAA
• Follow us on Twitter @HHSOCR
• Join our Privacy and Security listservs at https://www.hhs.gov/hipaa/for-professionals/list-serve/