HIPAA Enforcement:
Ongoing Patterns of Non-Compliance

Serena Mosley-Day

Senior Advisor

HIPAA Compliance and Enforcement

HHS Office for Civil Rights

March 4, 2019

General Enforcement Highlights

- Expect to receive over 26,000 complaints this year
- Receive over 350 500+ breach reports per year
- In most cases, entities able to demonstrate satisfactory compliance through voluntary cooperation and corrective action
- In some cases, the 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

As of January 31, 2019

Enforcement and Compliance Activities

- Complaint Investigations
- Compliance Reviews
  - Including all 500+ breach reports
- Letters of Finding
- Settlement Agreements
- Formal Enforcement
- Outreach and Public Education
- Audits

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

Breach Portal:
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Breach Reporting – What Should be Reported?

- "Acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the Privacy Rule] which compromises the security or privacy of the protected health information."
- 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

Breach Reports

- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
  - Public can search and sort posted breaches
    - 340 total 500 + breach reports 2016
    - 360 total 500 + breach reports 2017
    - 376 total 500 + breach reports 2018
- OCR opens investigations into breaches affecting 500+ individuals, and into a 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

2018 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

Lack of Business Associate Agreements

HIPAA generally requires that covered entities and business associates enter into agreements with their business associates (BAAs) to ensure that the business associates will appropriately safeguard protected health information.

(See 45 CFR §§ 164.502(e), 164.504(e), and 164.308(b)).

The HIPAA Omnibus Rule, issued in January 2013, changed the standards for BAAs

- –Modified BAA requirements
- –Must execute a BAA that includes the modified provisions
- –Compliance date: September 23, 2013

Case Example: Advanced Care Hospitalists

- A contractor physician group
- ACH filed a breach report confirming that ACH patient information was viewable on a medical billing services' website
- ACH never had a BAA with the individual providing medical billing services to ACH
- ACH failed to adopt any policy requiring business associate agreements until April 2014
- ACH had been in operation since 2005
  - No risk analysis or implemented security measures
  - No HIPAA policies or procedures before 2014.
- Settlement with RA/CAP - September 2018 for $500,000

Risk Analysis: Incomplete or Inaccurate

- Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization]. See 45 C.F.R. § 164.308(a)(1)(ii)(A).

Case Example: Anthem, Inc.

- Largest U.S. PHI breach in history.
  - 78.8 million individuals affected
- Failure to conduct an enterprise-wide risk analysis
- Found inadequate safeguards to prevent and address spearphishing attacks
- Settlement with RA/CAP – October, 2018 for $16,000,000

Impermissible Disclosures: Media

- A covered entity, including a health care provider, may not use or disclose protected health information (PHI), except either: (1) as the HIPAA Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.
- OCR Media Guidance
  - https://www.hhs.gov/hipaa/for-professionals/faq/2023/film-and-media/index.html

Case Example: Allergy Associates

- Dispute regarding care
- Impermissible Disclosure to reporter
- Advised by Privacy Officer and attorney not to discuss matter
- Disregarded advice
- Settlement with RA/CAP - November 2018 for $125,000

Case Example: ABC Cases

- Involved in filming of ABC television network documentary series
- Failed to first obtain authorization from patients

3 Separate Settlements - $999,000:

- Boston Medical Center ($100,000)
- Brigham and Women's Hospital ($384,000)
- Massachusetts General Hospital ($515,000)

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

Corrective Actions May Include:

- Updating risk analysis and risk management plans
- Updating policies and procedures
- Evaluating vendor/contractor relationships and updating BAAs
- Training of workforce
- External monitoring

Compliance Best Practices

- Review vendor/contractor relationships to ensure required BAAs are in place 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

Right of Access – Provider Education

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

Credits Available

Physicians - maximum of 0.50 *AMA PRA Category 1 Credit(s)™*

You Are Eligible For

- AMA PRA Category 1 Credit(s)™

Accreditation Statements

For Physicians

Medscape

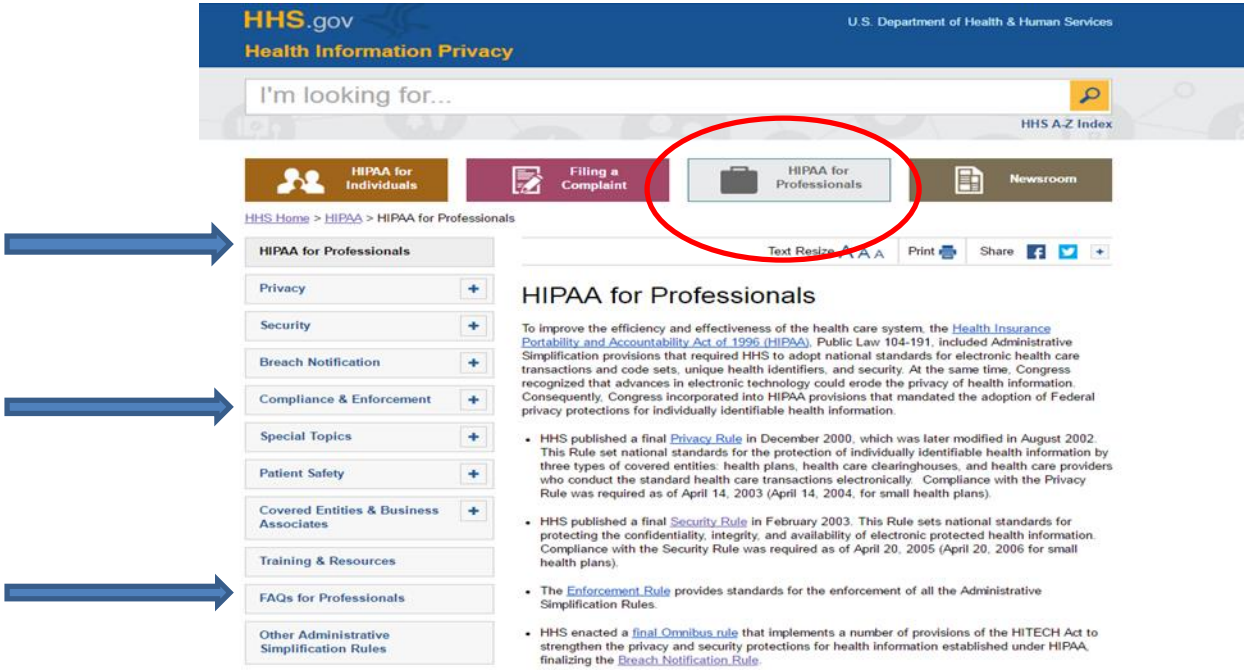
Medscape, LLC is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians.

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

For More Information



- OCR's website at https://www.hhs.gov/hipaa
- Join our Privacy and Security listservs at https://www.hhs.gov/hipaa/for-professionals/list-serve/
- Find us on Twitter @hhsocr