

The logo for HIMSS 18, featuring the word "Himss" in a sans-serif font and "18" in a large, bold, blue font.

The leading health information and technology conference

WHERE **THE WORLD** CONNECTS FOR HEALTH

Conference & Exhibition | March 5–9, 2018

Las Vegas | Venetian – Palazzo – Sands Expo Center

A HIPAA Compliance and Enforcement Update from the HHS Office for Civil Rights

Session #24, 10:00 a.m. – 11:00 a.m. March 6, 2018

Roger Severino, MSPP, JD

Director, HHS Office for Civil Rights

Nicholas Heesters, MEng, JD, CIPP

Health Information Privacy & Security Specialist,

HHS Office for Civil Rights

COMMITMENT

www.himssconference.org



#HIMSS18

U.S. DEPARTMENT OF
HEALTH AND HUMAN SERVICES

**OFFICE FOR
CIVIL RIGHTS**

DISCLAIMER: The views and opinions expressed in this presentation are those of the author and do not necessarily represent official policy or position of HIMSS.

Conflict of Interest

Roger Severino, MSPP, JD

Nicholas Heesters, MEng, JD, CIPP

Have no real or apparent conflicts of interest to report.

Agenda

- Recent HIPAA Enforcement
- Breach Notification Highlights
- Technical Assistance and Education

Learning Objectives

- Describe recent HIPAA enforcement actions and recognize patterns of noncompliance
- Identify best practices for HIPAA compliance
- Explain the importance of risk analysis and other strategies for an effective HIPAA compliance program

RECENT HIPAA ENFORCEMENT AND BREACH HIGHLIGHTS

General HIPAA Enforcement Highlights as of April 14, 2003 – January 31, 2018

- Over 173,426 HIPAA complaints received to date
- Over 25,695 HIPAA cases resolved with corrective action and/or technical assistance
- Expect to receive over 24,000 HIPAA complaints this year

Enforcement, cont.

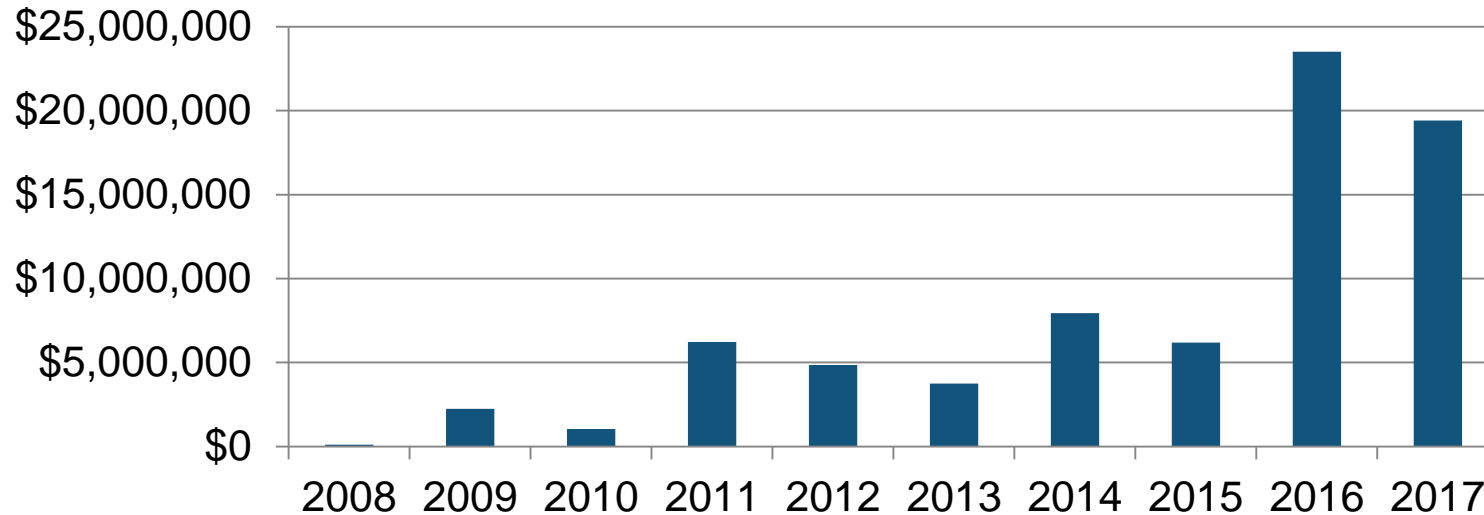
- In most cases, entities are able to demonstrate satisfactory compliance through voluntary cooperation and corrective action during the investigation
- In some cases though, the nature or scope of indicated noncompliance warrants additional enforcement action
- Resolution Agreements/Corrective Action Plans
- 52 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 3 civil money penalties

HIPAA Enforcement since HIMSS17

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

Total \$11,618,200

HIPAA Resolution Agreements and CMPs



50 settlement agreements and 3 civil money penalties through 2017

Recurring Compliance Issues

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

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 external monitoring

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

New HIPAA Breach Reporting Tool

- The revised web tool still publicly reports all breaches involving 500 or more records – but presents that information in a more understandable way.
- The HBRT also features improved navigation for both those looking for information on breaches and ease-of-use for organizations reporting incidents.
- The tool helps educate industry on the types of breaches that are occurring, industry-wide or within particular sectors, and how breaches are commonly resolved following investigations launched by OCR, which can help industry improve the security posture of their organizations.

U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

Welcome | File a Breach | HHS | Office for Civil Rights | Contact Us

Indicates active cases under investigation within last 24 months

Please Note: The Breach Notification is required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information if the following breaches have been reported to the Secretary:

Cases Currently Under Investigation
This page lists all breaches reported within the last 24 months

Under Investigation | Archive | Help for Consumers

Help for consumers provides tools on identity theft

Archive tab takes users to OCR's database of all breach cases

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

Advanced Search Function

Under Investigation Archive Help for Consumers

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting

Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

[Hide Advanced Options](#)

Breach Submission Date: From: To:

Type of Breach:

<input type="checkbox"/> Hacking/IT Incident	<input type="checkbox"/> Improper Disposal	<input type="checkbox"/> Loss
<input type="checkbox"/> Theft	<input type="checkbox"/> Unauthorized Access/Disclosure	<input type="checkbox"/> Unknown
<input type="checkbox"/> Other		

Location of Breach:

<input type="checkbox"/> Desktop Computer	<input type="checkbox"/> Electronic Medical Record	<input type="checkbox"/> Email
<input type="checkbox"/> Laptop	<input type="checkbox"/> Network Server	<input type="checkbox"/> Other Portable Electronic Device
<input type="checkbox"/> Paper/Films	<input type="checkbox"/> Other	

Type of Covered Entity:

State:

Business Associate Present?:

Description Search:

CE / BA Name Search:

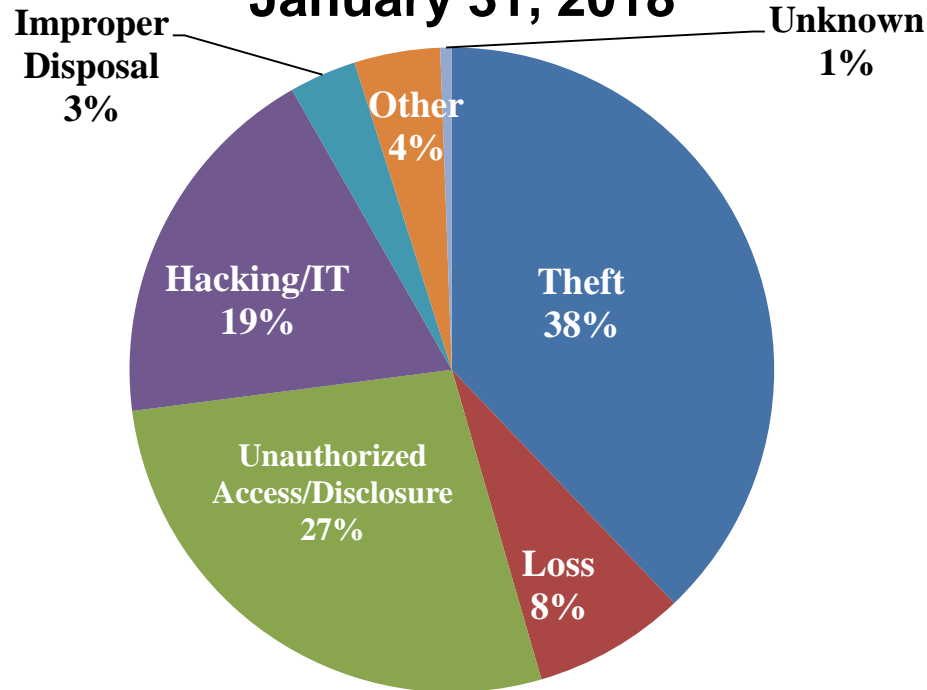
Apply Filters

Latest Breach Reporting Highlights

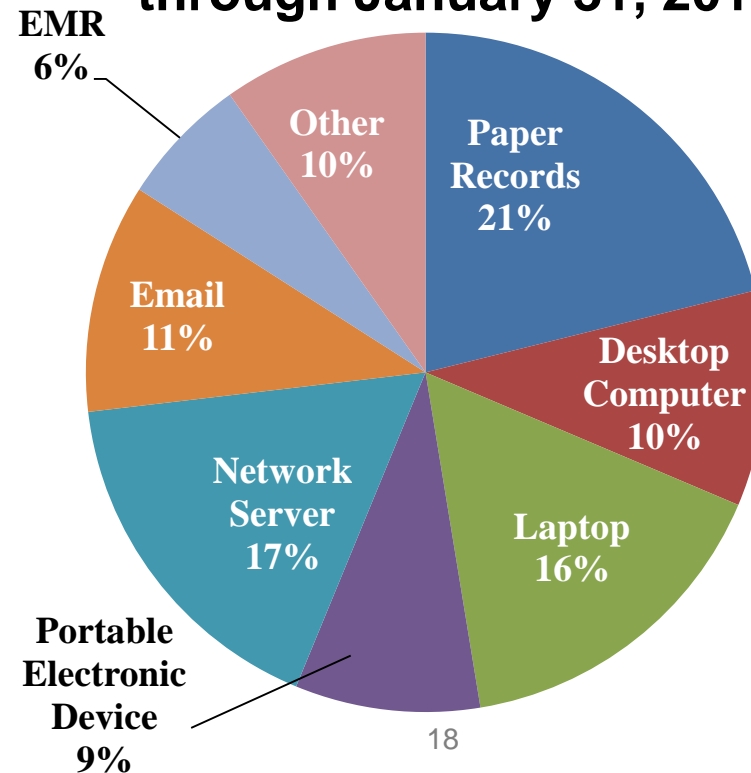
September 2009 through January 31, 2018

- Over 2,200 reports involving a breach of PHI affecting 500 or more individuals
- Type:
 - Theft makes up 38% of large breaches
 - Hacking/IT now accounts for 19% of incidents
- Location:
 - Laptops and other portable storage devices account for 25% of large breaches
 - Paper records are 21% of large breaches
- Individuals affected are approximately 177,065,101
- Over 316,000 reports of breaches of PHI affecting fewer than 500 individuals

500+ Breaches by Type of Breach from September 2009 through January 31, 2018



500+ Breaches by Location of Breach from September 2009 through January 31, 2018



Technical Assistance and Education

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, and OCR considers comments as we develop our priorities for additional guidance and technical assistance
- Approximately 900 to 1,200 visitors per month

Find it at <http://hipaaQsportal.hhs.gov>

The screenshot shows the homepage of the HIPAA Qsportal. At the top, the U.S. Department of Health and Human Services logo and the Office for Civil Rights logo are displayed on the left. The main heading reads "Health app developers, what are your questions about HIPAA?". Below this is a navigation bar with links: Welcome, About, Open Qs, Answered Qs, Helpful Links, Notes, and Contact. The main content area is divided into two columns. The left column, titled "HIPAA Health Information Privacy, Security and Breach Notification Rules", contains three yellow buttons: "About HIPAA", "Health App Use Scenarios & HIPAA", and "Guidance on HIPAA & Cloud Computing". The right column, titled "Engage with OCR on issues & concerns related to protecting health information privacy in mHealth design and development", contains a single yellow button: "Submit & View Questions". At the bottom center, there is a blue button labeled "About".

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

Health app developers, what are your questions about HIPAA?

Welcome About Open Qs Answered Qs Helpful Links Notes Contact

HIPAA Health Information Privacy, Security and Breach Notification Rules

About HIPAA

Health App Use Scenarios & HIPAA

Guidance on HIPAA & Cloud Computing

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

Submit & View Questions

About

Recently Answered Questions

- When are health app developers subject to HIPAA?
- What safeguards for PHI are needed for offline devices?
- What are suggested encryption protocols for cloud security?
- Which video chat apps are HIPAA compliant?
- Are we a HIPAA compliant distributed team?
- Does HIPAA require scanning and penetration testing?
- Can patients request controlled access or data masking in EHRs?
- What activity within an application must be logged?
- How should developers execute audit logging?

Cyber-Attack Quick Response

Experienced a ransomware attack or other cyber-related security incident?
This Cyber-Attack Quick Response guide will explain steps that a HIPAA covered entity or its business associate should take to respond.



RESPOND

The entity must execute response and mitigation procedures, and contingency plans.



REPORT CRIME

The entity should report the crime to criminal law enforcement agencies.



REPORT THREAT

The entity should report all cyber threat indicators to the appropriate federal agencies and ISAOs.



ASSESS BREACH

The entity must assess the incident to determine if there is a breach of protected health information.

IF YES

Is there a breach?

IF NO

All breaches must be reported to the affected individuals no later than 60 days from occurrence. If the breach affects 500 or more individuals, the entity must report to OCR and the media as soon as possible, but no later than 60 days from the occurrence. If the breach affects fewer than 500 individuals, the entity must report to OCR no later than 60 days after the calendar year of the breach.

The entity must document and retain all information considered during the risk assessment of the cyber-attack, including how it determined no breach occurred.

Cyber Security Guidance Material

Ransomware

- Following the May 2017 WannaCry ransomware attack, HHS reminded organizations to adhere to the OCR ransomware guidance as part of strong cyber hygiene.
- OCR presumes a breach in the case of a ransomware attack.

FACT SHEET: Ransomware and HIPAA

<https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>


“Maintaining frequent backups and ensuring the ability to recover data from backups is crucial to recovering from a ransomware attack.”

Cybersecurity Newsletters

- Launched in 2016
- Recent Newsletters
 - 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>

New: Free Continuing Medical Education and Continuing Education Credit via Medscape for Health Care Providers



THUMBNAILS

An Individual's Right to Access and Obtain Their Health Information Under HIPAA

Moderator
Deven McGraw, JD, MPH
Deputy Director for Health Information Privacy
Office for Civil Rights
US Department of Health and Human Services
Washington, DC

Developed as part of a Medscape education activity, *An Individual's Right to Access and Obtain Their Health Information Under HIPAA*, supported by the US Department of Health and Human Services.

IN THIS PRESENTATION

- Introduction
- HIPAA Privacy Rule Overview
- Scope of Information
- Form, Format & Access

NEXT >

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

Questions?

<http://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

Please complete the online session evaluation