



Developments in HIPAA and Related Issues in Health Information Law (that You Can't Learn from ChatGPT)

*MaHIMA Dot Wagg Memorial Legislative Seminar
November 3, 2023*

Colin J. Zick, Esq.
Foley Hoag LLP

Colin J. Zick

Partner and Co-Chair, Health Care and Privacy & Data Security Practice Groups
Boston | +1.617.832.1275 | czick@foleyhoag.com



- Counsels clients ranging from the Fortune 1000 to start-ups on issues involving information privacy and security, including state, federal and international data privacy and security laws and government enforcement actions.
- Advises on issues involving the transfer of data between jurisdictions, including GDPR, EU-US Privacy Shield, CCPA, CPRA, and other data privacy and security laws, cloud security, cyber insurance, the Internet of Things, and data breach response.
- Co-founded the firm's Privacy and Data Security Group (which he currently chairs) and regularly contributes to its "Security, Privacy and the Law" blog, www.securityprivacyandthelaw.com. Serves as a member of Law360's Privacy & Consumer Protection editorial advisory board.
- Selected by his peers for inclusion in THE BEST LAWYERS IN AMERICA in the fields of Healthcare Law (2015-present) and Privacy and Data Security (2018-present)
- Ranked by CHAMBERS USA: AMERICA'S LEADING LAWYERS FOR BUSINESS as one of Massachusetts' leading Healthcare attorneys (2010-present)

- *How has privacy/security for health information changed post-COVID?*
- *HIPAA and Cybersecurity – Hacking on the rise*
- *What is the impact of AI on privacy/security and related regulations?*
- *What new laws, regulations, and court cases impact health information?*

- *How has privacy/security for health information changed post-COVID?*

- The COVID-19 pandemic dramatically changed the delivery of health care
- At-home/decentralized care is now where it's at:
 - Telehealth
 - Self-testing
 - Vaccines at your local pharmacy
- More and more of us are wearing devices that monitor aspects of our health
- More and more providers are connected by EHRs
- Ransomware has become an organized business
- AI is everywhere, in everything
- But HIPAA has not changed:
 - Telehealth prospers because HIPAA was not enforced
 - Self-testing is not necessarily covered by HIPAA
 - Our device data is not covered by HIPAA
 - De-identified data that is feeding AI is not covered by HIPAA

OCR HIPAA Announcements Related to COVID-19:

- [OCR Issues Guidance on HIPAA, COVID-19 Vaccinations, and the Workplace - September 30, 2021](#)
- [OCR Announces Notification of Enforcement Discretion for Use of Online or Web-Based Scheduling Applications for the Scheduling of COVID-19 Vaccination Appointments – January 19, 2021](#)
- [OCR Issues Guidance on HIPAA, Health Information Exchanges, and Disclosures of Protected Health Information for Public Health Purposes - December 18, 2020](#)
- [Trump Administration Adds Health Plans to June 2020 Plasma Donation Guidance - August 24, 2020](#)
- [OCR Issues Guidance on How Health Care Providers Can Contact Former COVID-19 Patients About Blood and Plasma Donation Opportunities - June 12, 2020](#)
- [OCR Issues Guidance on Covered Health Care Providers and Restrictions on Media Access to Protected Health Information about Individuals in Their Facilities - May 5, 2020](#)
- [OCR Announces Notification of Enforcement Discretion for Community-Based Testing Sites During the COVID-19 Nationwide Public Health Emergency - April 9, 2020](#)
- [OCR Announces Notification of Enforcement Discretion to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities During The COVID-19 Nationwide Public Health Emergency - April 2, 2020](#)
- [OCR Issues Bulletin on Civil Rights Laws and HIPAA Flexibilities That Apply During the COVID-19 Emergency - March 28, 2020](#)
- [OCR Issues Guidance to Help Ensure First Responders and Others Receive Protected Health Information about Individuals Exposed to COVID-19 - March 24, 2020](#)
- [OCR Issues Guidance on Telehealth Remote Communications Following Its Notification of Enforcement Discretion - March 20, 2020](#)
- [OCR Announces Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency - March 17, 2020](#)

■ Notifications of Enforcement Discretion

- [Notification of Enforcement Discretion for Use of Online or Web-Based Scheduling Applications for the Scheduling of COVID-19 Vaccination Appointments - PDF](#)
- [Notification of Enforcement Discretion for Community-Based Testing Sites - PDF](#)
- [Notification of Enforcement Discretion for Business Associates - PDF](#)
- [Notification of Enforcement Discretion for Telehealth - PDF](#)

- [Guidance on HIPAA, COVID-19 Vaccination, and the Workplace - September 30, 2021](#)
- [Guidance on HIPAA, Health Information Exchanges, and Disclosures of Protected Health Information for Public Health Purposes – December 18, 2020 - PDF*](#)
- [Updated Guidance on HIPAA and Contacting Former COVID-19 Patients about Plasma Donation - August 2020 - PDF*](#)
- [Guidance on Covered Health Care Providers and Restrictions on Media Access to Protected Health Information about Individuals in Their Facilities - PDF](#)
- [Disclosures of PHI to Law Enforcement, Paramedics, Other First Responders and Public Health Authorities - PDF*](#)
- [FAQs on HIPAA and Telehealth - PDF](#)

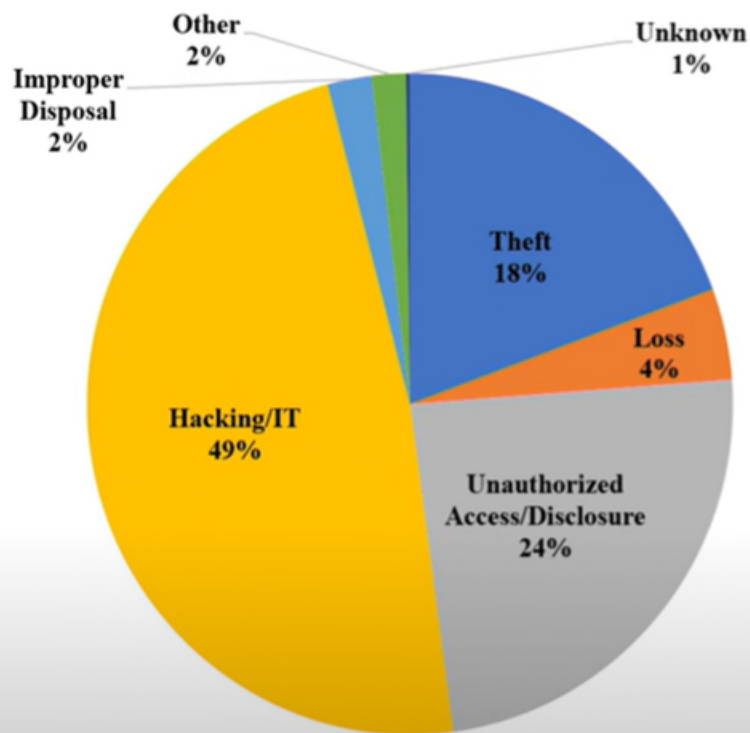
- *HIPAA and Cybersecurity – Hacking on the rise*

HIPAA and Cybersecurity

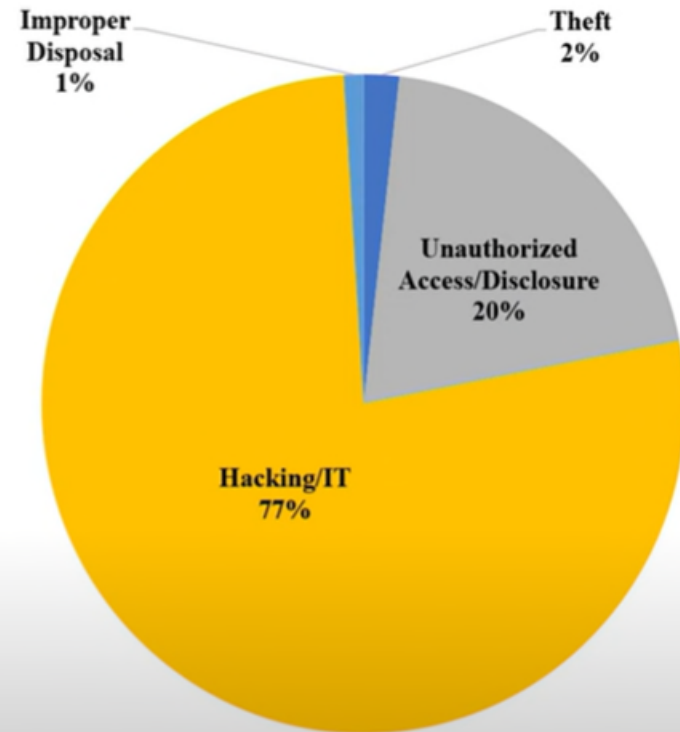
- 239% increase in Hacking/IT Incident large breaches from 2018 to 2022
- 278% increase in Ransomware large breaches from 2018 to 2022
- Common Attack Vectors
 - Phishing
 - Compromised accounts (remote access)
 - Unpatched vulnerabilities
- HIPAA Security Rule Can Help Prevent, Defend, Mitigate, and Recover
 - Security Awareness and Training
 - Authentication
 - Access Control
 - Risk Analysis / Risk Management

Source: HHS OCR How the HIPAA Security Rule Can Help Defend Against Cyber-Attacks | October 23, 2023

500+ Breaches by Type of Breach



September 23, 2009 through Dec 31, 2022

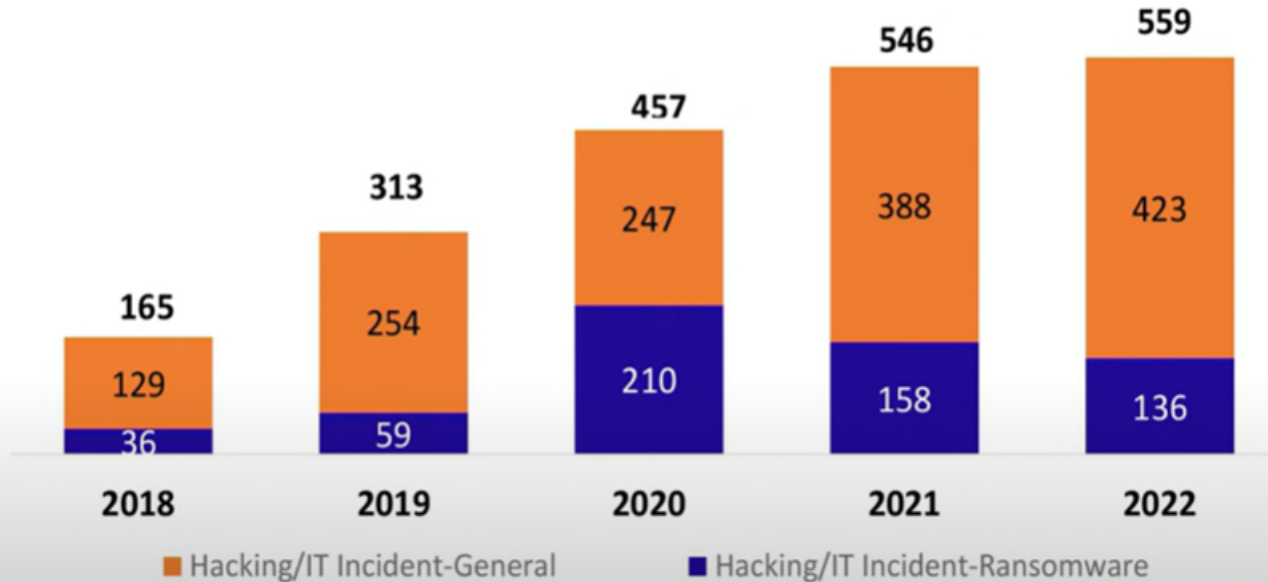


January 1, 2023 through September 30, 2023

Source: HHS OCR How the HIPAA Security Rule Can Help Defend Against Cyber-Attacks | October 23, 2023

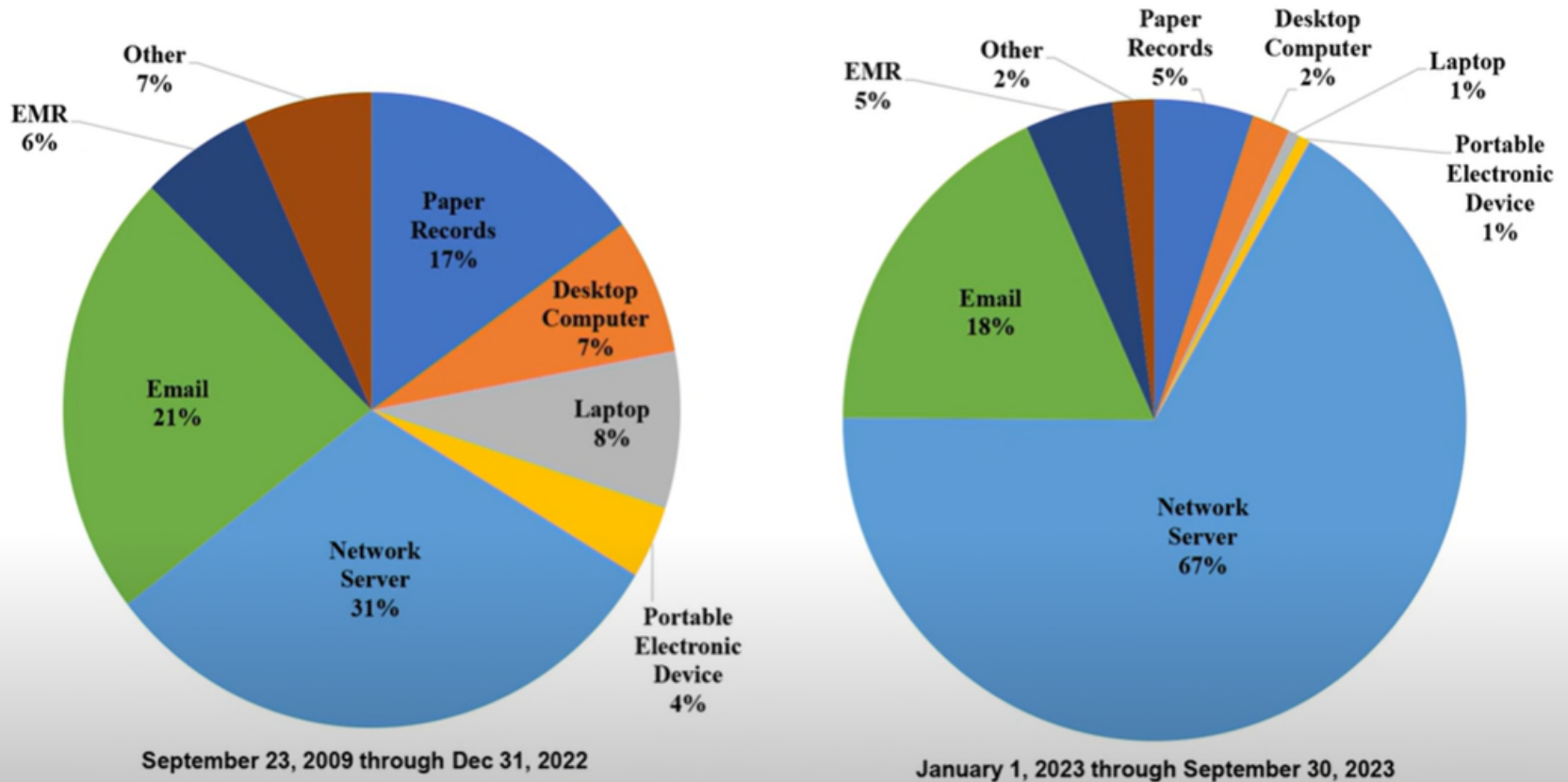
Breaches Affecting 500 or More Individuals Reports Received Involving Hacking/IT Incidents

Calendar Years 2018 - 2022



Source: HHS OCR How the HIPAA Security Rule Can Help Defend Against Cyber-Attacks | October 23, 2023

500+ Breaches by Location of Breach



Source: HHS OCR How the HIPAA Security Rule Can Help Defend Against Cyber-Attacks | October 23, 2023

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 500 or more individuals. The following breaches have been reported to the Secretary:

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.

[Show Advanced Options](#)

Breach Report Results							
Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
☐	Ryders Health Management LLC	CT	Healthcare Provider	7252	09/07/2023	Hacking/IT Incident	Network Server
☐	Roseman University of Health Sciences	NV	Healthcare Provider	4622	09/06/2023	Hacking/IT Incident	Network Server
☐	Amerita	KS	Healthcare Provider	219707	09/05/2023	Hacking/IT Incident	Network Server
☐	Delta Dental of California	CA	Health Plan	500	09/05/2023	Hacking/IT Incident	Network Server
☐	Bloom Health Centers	MD	Healthcare Provider	1545	09/01/2023	Unauthorized Access/Disclosure	Email
☐	North Mississippi Medical Center, Inc.	MS	Healthcare Provider	950	09/01/2023	Hacking/IT Incident	Email
☐	MedMinder Systems, Inc.	MA	Healthcare Provider	12146	09/01/2023	Hacking/IT Incident	Network Server
☐	Enzo Clinical Labs, Inc.	NY	Healthcare Provider	1700	08/31/2023	Hacking/IT Incident	Network Server
☐	Mountain View Family Practice, PC	MA	Healthcare Provider	5139	08/31/2023	Hacking/IT Incident	Electronic Medical Record, Network Server
☐	Indiana University Health	IN	Health Plan	1191	08/31/2023	Hacking/IT Incident	Network Server
☐	TTEC Healthcare Solutions	CO	Business Associate	2953	08/30/2023	Unauthorized Access/Disclosure	Other
☐	O'Neil Digital Solutions, LLC	CA	Business Associate	1722	08/30/2023	Unauthorized Access/Disclosure	Paper/Films
☐	PurFoods, LLC	IA	Healthcare Provider	1229333	08/25/2023	Hacking/IT Incident	Network Server
☐	Associates in Pediatric Dentistry	LA	Healthcare Provider	9703	08/25/2023	Hacking/IT Incident	Email
☐	Data Media Associates	GA	Business Associate	74730	08/24/2023	Hacking/IT Incident	Other
☐	Detroit Central City Community Mental Health	MI	Healthcare Provider	1412	08/24/2023	Hacking/IT Incident	Email
☐	IEC Group, Inc. dba AmeriBen	ID	Business Associate	74884	08/24/2023	Unauthorized Access/Disclosure	Email
☐	Milan Eye Center	GA	Healthcare Provider	67336	08/23/2023	Hacking/IT Incident	Network Server
☐	PRIME THERAPEUTICS LLC	MN	Business Associate	6050	08/23/2023	Hacking/IT Incident	Network Server
☐	Vecino Health Centers	TX	Healthcare Provider	1339	08/22/2023	Hacking/IT Incident	Network Server
☐	Serco Inc. Group Health Plan	VA	Health Plan	10140	08/22/2023	Hacking/IT Incident	Network Server
☐	Absolute Dental Services	NC	Business Associate	10037	08/21/2023	Hacking/IT Incident	Email
☐	McAlester Regional Health Center	OK	Healthcare Provider	500	08/21/2023	Hacking/IT Incident	Desktop Computer, Network Server
☐	The University of Massachusetts Chan Medical School	MA	Business Associate	134394	08/21/2023	Hacking/IT Incident	Network Server

Data Breach Notification Letters September 2023

Below find copies of data breach notification letters sent to consumers impacted by a data breach.



Assigned Data Breach Number - 28911 - Jackson Lewis (English, PDF 286.1 KB)



Assigned Data Breach Number - 29106 - Elevate Services, Inc. (Additional Information)
(English, PDF 235.98 KB)



Assigned Data Breach Number - 29313 - TMX Finance Corporate Services, Inc. (Additional Information) (English, PDF 274.16 KB)



Assigned Data Breach Number - 29410 - Traditions Bancorp, Inc. (Additional Information)
(English, PDF 576.86 KB)



Assigned Data Breach Number - 29610 - R&B Credit Control Corporation of Virginia d/b/a Credit Control Corporation (Additional Information) (English, PDF 255.57 KB)



Assigned Data Breach Number - 29621 - Osiac (formerly Advisor Group) (Additional Information) (English, PDF 869.8 KB)



Assigned Data Breach Number - 29767 - Harvard Pilgrim Health Care (Additional Information) (English, PDF 114.17 KB)

- *What is the impact of AI on privacy/security and related regulations?*

- Citizens are voicing concerns about harms related to AI—and their concerns span the technology’s lifecycle, from how it’s built to how its applied by third parties in the real world. In this piece, we summarize a few key areas of harm we reviewed.
- AI models require massive amounts of data for training.
- Concerns About How AI Works and Interacts with Users: Bias and inaccuracies
 - AI models are susceptible to bias, inaccuracies, “hallucinations,” and bad performance.
 - AI model accuracy is dependent on a number of factors including the input data, training techniques, and context of deployment.
 - AI applications are designed to be efficient (using less resources, while yielding more output) in order to optimize for scalability and profit. This often means reducing the number of humans involved, leaving consumers to engage with their AI replacements.
- Limited pathways for appeal and bad customer service (AKA can we talk to a human please)
- Concerns About How AI is Applied in the Real World: Misuse, fraud, and scams.
 - Phishing emails will become hard to spot as scammers start to write them with generative AI products and previously tell-tale spelling and grammar mistakes disappear.
 - AI can be used to conduct sophisticated voice cloning scams, in which family members’ or loved ones’ voices are used for financial extortion. Some even say they’ve already experienced this themselves.
 - Similarly, romance scams and financial fraud could be turbo-charged by generative AI, as scammers use chatbot products to communicate with more people at a lower cost. Many reports described being tricked by such scams and expressing a belief the messages originated from an AI model.

Concerns About How AI is Applied in the Real World: Misuse, fraud, and scams.

- Concerns About How AI is Applied in the Real World: Misuse, fraud, and scams.
 - Phishing emails will become hard to spot:
 - scammers start to write them with generative AI products
 - previously tell-tale spelling and grammar mistakes disappear.
 - AI can be used to conduct sophisticated voice cloning scams:
 - family members' or loved ones' voices are used for financial extortion.
 - Similarly, romance scams and financial fraud could be turbo-charged by generative AI:
 - scammers use chatbot products to communicate with more people at a lower cost.
 - Many reports described being tricked by such scams and expressing a belief the messages originated from an AI model.

Ransomware Resources

HHS Health Sector Cybersecurity Coordination Center Threat Briefs and Sector Alerts:

- <https://www.hhs.gov/about/agencies/asa/ocio/hc3/products/index.html>

Section 405(d) of the Cybersecurity Act of 2015 Resources:

- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients <https://405d.hhs.gov/information>
- 405(d) Products, Publications and Materials <https://405d.hhs.gov/resources>

OCR Guidance:

- Ransomware <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>
- Cybersecurity <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html>
- Risk Analysis <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf>

HHS Security Risk Assessment Tool: <https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool>

CISA Resources:

- <https://www.cisa.gov/stopransomware>
- https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf
- https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf

FBI Resources:

- <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware>
- <https://www.ic3.gov/Media/Y2019/PSA191002>

Source: HHS OCR How the HIPAA Security Rule Can Help Defend Against Cyber-Attacks | October 23, 2023

- *What new laws, regulations, and court cases impact health information?*

Key elements of the proposed MIPS

- Applies to non-HIPAA “personal information”
- Similar in many respects to newish laws in California, Colorado, Virginia, and Connecticut
- Would apply to entities with revenues exceeding \$25M per year; determines the processing of at least 100,000 individuals; or is a data broker.

What would change?

- Far broader scope of information covered than HIPAA or existing Massachusetts law
- Risk assessments
- Private right of action

- Gardner, Massachusetts based Heywood Healthcare **cited** a "lengthy electronic medical record transition" as a factor in its decision to file for Chapter 11 bankruptcy protection.
- In 2019, Heywood was one of several Massachusetts health systems that **opted** for Meditech Expanse as its EHR vendor. Meditech is based out of nearby Canton, Mass. Heywood Healthcare did not respond to *Becker's* request for comment.

https://www.beckershospitalreview.com/ehrs/massachusetts-health-system-cites-costly-ehr-transition-in-bankruptcy-decision.html?origin=CIOE&utm_source=CIOE&utm_medium=email&utm_content=newsletter&oly_enc_id=1905F7435578H3V

Is It Customer Services or a HIPAA Violation?

From Modern Healthcare:

- A patient publicly criticized CVS Health, its executives and Caremark, its pharmacy benefit manager, for requiring her and other commercial enrollees to switch from Bristol-Myers Squibb's Eliquis to Janssen Pharmaceuticals' Xarelto, both anticoagulants that experts say have not been proven interchangeable through randomized control trials. Observational studies have concluded the two are not the same.
- The patient tagged the company and several of its executives, including its CEO, in multiple Twitter posts. She called out the business during public testimony before the Federal Trade Commission.
- Then she received an unexpected call from a CVS employee, who said he wanted to talk about her health history. It raises the question: by using information from her private Caremark account to perform customer service, were the federal laws on the disclosure of patient information violated?

LA Care, the largest publicly operated health plan in the country paid \$1,300,000 to settle HIPAA security allegations.

- The potential violations in this case included the following failures:
 - To conduct an accurate and thorough **risk analysis** to determine risks and vulnerabilities to ePHI,
 - To **implement security measures** to reduce risks/vulnerabilities to ePHI to a reasonable and appropriate level,
 - To implement sufficient procedures to **regularly review records of information system activity**,
 - To perform a **periodic technical and nontechnical evaluation** in response to environmental or operational changes affecting the security of ePHI, and
 - To **implement hardware, software, and/or procedural mechanisms** that record and examine activity in information systems that contain or use ePHI.
- In addition to the monetary settlement, LA Care has agreed to take the following steps under a comprehensive corrective action plan that will be monitored for three years by OCR to ensure compliance with HIPAA:
 - Conduct an accurate and thorough **risk analysis** to determine risks and vulnerabilities to electronic patient/system data across the organization.
 - Develop and implement a **risk management plan** to address identified risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.
 - Develop, implement, and distribute **policies and procedures** for a risk analysis and risk management plan.
 - **Report** to HHS when it conducts an **evaluation due to an environmental and operational** change that affects the security of ePHI in LA Care's possession or control.
 - **Report** to HHS within thirty (30) days when workforce members **fail to comply** with the HIPAA Rules.

- CCPA went into effect January 1, 2020; it regulates the privacy of health information of California residents, but exempts:
 - Protected Health Information (PHI)
 - Personal information that HIPAA-covered entities handle like PHI
 - Most likely to benefit from this exemption
 - Health care providers
 - Health insurers
 - These companies collect personal information that is not exempt:
 - Employment information
 - Electronic network activity information (e.g., cookies)
 - Labs doing return to work COVID screening (not diagnostic testing)
- More laws like this have followed, e.g., Washington, and will continue to follow.

- **JOHN DOE, et al., Plaintiff, v. ATRIUS HEALTH, INC., Defendant.**
- **Civil Action No. 22-12196-FDS**
 - ***MEMORANDUM AND ORDER ON PLAINTIFFS' MOTION TO REMAND***
- **SAYLOR, C.J.**
 - This is a putative class action against a non-governmental healthcare provider alleging systematic violation of patients' state-law privacy rights. The complaint was originally filed in the Norfolk County Superior Court before being removed to federal court under 28 U.S.C. § 1442(a)(1). Plaintiffs have moved to remand, contending that federal subject-matter jurisdiction is lacking because defendant has failed to meet the requirements of § 1442(a)(1). For the reasons set forth below, the motion to remand will be granted.
 - **I. Background**
 - **A. Factual Background**
 - Atrius Health, Inc. is the parent company for more than 30 medical practices in Massachusetts. (Compl. ¶8). Its principal place of business is in Massachusetts, and it is a Massachusetts corporation. (*Id.*). Atrius operates websites designed for patient communications, scheduling, searching for physicians, paying bills, requesting medical records, learning about medical issues, and joining support groups. (*Id.* ¶¶19-20).
 - The complaint alleges that plaintiffs visited defendant Atrius's websites in 2022 and entered data, including personal health information. (*Id.* ¶¶88, 91). The complaint alleges that Atrius's websites utilized Facebook's Meta Pixel tool—a computer code that tracks users' activities on a website, allowing that information to be processed and analyzed by Facebook and shared with third-party advertisers. (*Id.* ¶¶54-56, 92).

■ *John Doe 1 and John Doe 2 v. Boston Medical Center*

**MEMORANDUM OF DECISION AND ORDER ON
DEFENDANT’S MOTION TO DISMISS**

Plaintiffs John Doe 1 and John Doe 2 commenced this putative class action against defendant Boston Medical Center Corporation (“BMC”), alleging that it used digital marketing tools on its website that illegally redirected website users’ personal information, and the contents of their communications with BMC’s website, to third parties Google and Meta. On the basis of these allegations, the Complaint asserts claims for violations of the Massachusetts Wiretap Statute, G.L. c. 272, § 99, and invasion of privacy under G. L. c. 214, § 1B. Presently before the court is BMC’s motion to dismiss. After a hearing on July 18, 2023, and consideration of the parties’ submissions, the motion is **DENIED**.



Colin Zick

*Partner,
Co-Chair, Privacy & Data Security Practice*
Foley Hoag LLP

czick@foleyhoag.com | 617.832.1275