Health Care Data Breaches

Impacts and Lessons Learned from Security Incidents in Maryland and the Nation

DRAFT

APRIL 17, 2025

Background – Federal Requirements

- The Breach Notification Rule (rule) requires covered entities (CE) and business associates (BA) to report all breaches to the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) – part of HIPAA as amended by HITECH, effective September 2009
  - A breach is the impermissible acquisition, access, use, or disclosure of protected health information (PHI) that compromises the security or privacy of that information
  - The rule is applicable to breaches of substance use disorder records (Part 2) – effective April 2024
- The Federal Trade Commission (FTC) Health Breach Notification Rule requires entities that experience a breach and are not covered by HIPAA to notify affected consumers, the FTC, and, in some cases, the media

Breach Analysis

MARYLAND Health Care Commission

Randolph S. Sergent, Esq., Chairman
David Sharp, Acting Executive Director

Health Care Data Breaches

Impacts and Lessons Learned from Security Incidents in Maryland and the Nation

April 2025

INTRODUCTION

Data-theft crimes and ransomware attacks[1] against the health care sector are commonplace. Cyber risks extend across the various entities that make up the health care sector, including hospitals, medical practices, payers, pharmacies, labs, technology vendors, third-party contractors, and governments.[2] Protecting this essential health care ecosystem requires robust and adaptive cybersecurity approaches to safeguard patient health and financial data and maintain health care operations. Approaches include the implementation of "zero trust," a security framework where policies enforce a never trust, always verify principle.[3] Adoption of zero trust enables health care organizations to strengthen cybersecurity posture for how data is accessed and by whom to reduce the risk of a data breach.[4] The best security measures do not make organizations immune to cyber threats. Over the last decade, the health care sector has experienced a surge in reported data breaches of 500 or more records (Figure 1/Appendix A). The increased rate of breaches is attributed to the proliferation of cybercrime with a national average of 1.7 breaches reported daily from 2018-2024.[5]

Figure 1: Health Care Data Breaches
Nation, 2010-2024

Note: A large majority of records (>50 percent) is attributed to an Anthem data breach in 2015, MOVEit and other third-party breaches in 2023, and Change Healthcare in 2024.

1

- Data was analyzed from OCR's public use file on reported breaches affecting >500 individuals from January 1, 2010 through December 31, 2025
  - The analysis centered on breach occurrences by state (i.e., the location of the reporting CE or BA), type of breach, records, and reporting entity from 2021 to 2024
- Analyzing patterns and trends in breach data over time informs awareness building of factors that cause data breaches, impacts on consumer privacy, and the consideration of policies for improving data security
- Observations from the analysis and findings from literature are included in a written spotlight

Cohort of States

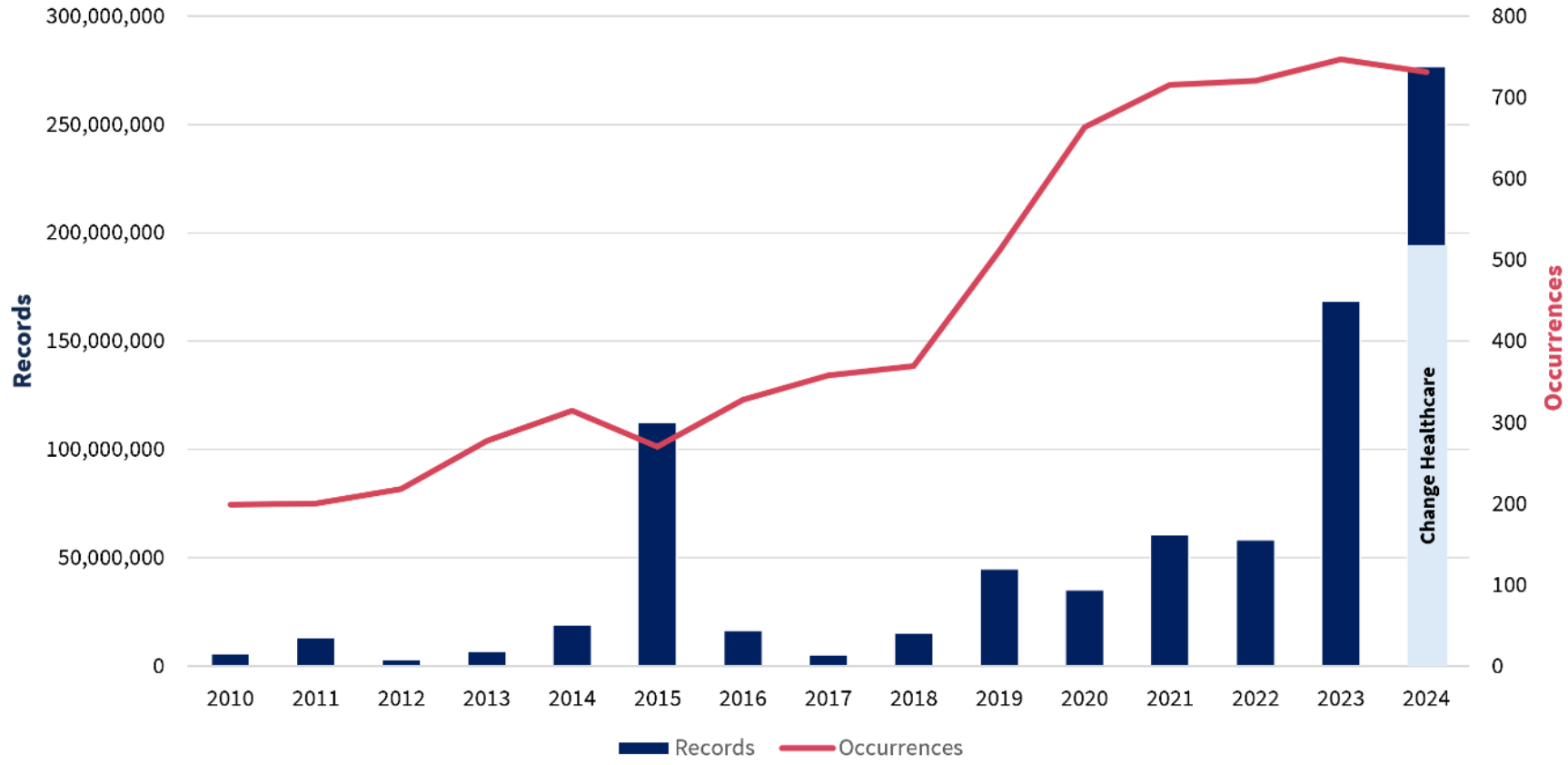
The breach analysis looked at states within 10 percent of Maryland for hospital inpatient days per capita* (2020-2022)

- Arizona
- Maryland
- Minnesota
- Mississippi
- New Hampshire
- Nevada
- Oklahoma
- Texas
- Virginia
- Vermont
- Wisconsin

**for every 100,000 people in the population*

Overall Snapshot of Breaches

Figure 1: Health Care Data Breaches
Nation, 2010-2024



Reporting Obligations/Considerations

- HIPAA requires a BA to notify the applicable CE when a breach occurs at or by the BA
  - CEs may delegate reporting responsibilities to the BA
- OCR has mechanisms to identify and prevent duplicate reports
- Multiple reported breaches may be linked to the same underlying security failure
- Major incidents (e.g., the Change Healthcare breach) are reported on behalf of many CEs affected

Breach Trends, 2021-2024

Key Observations

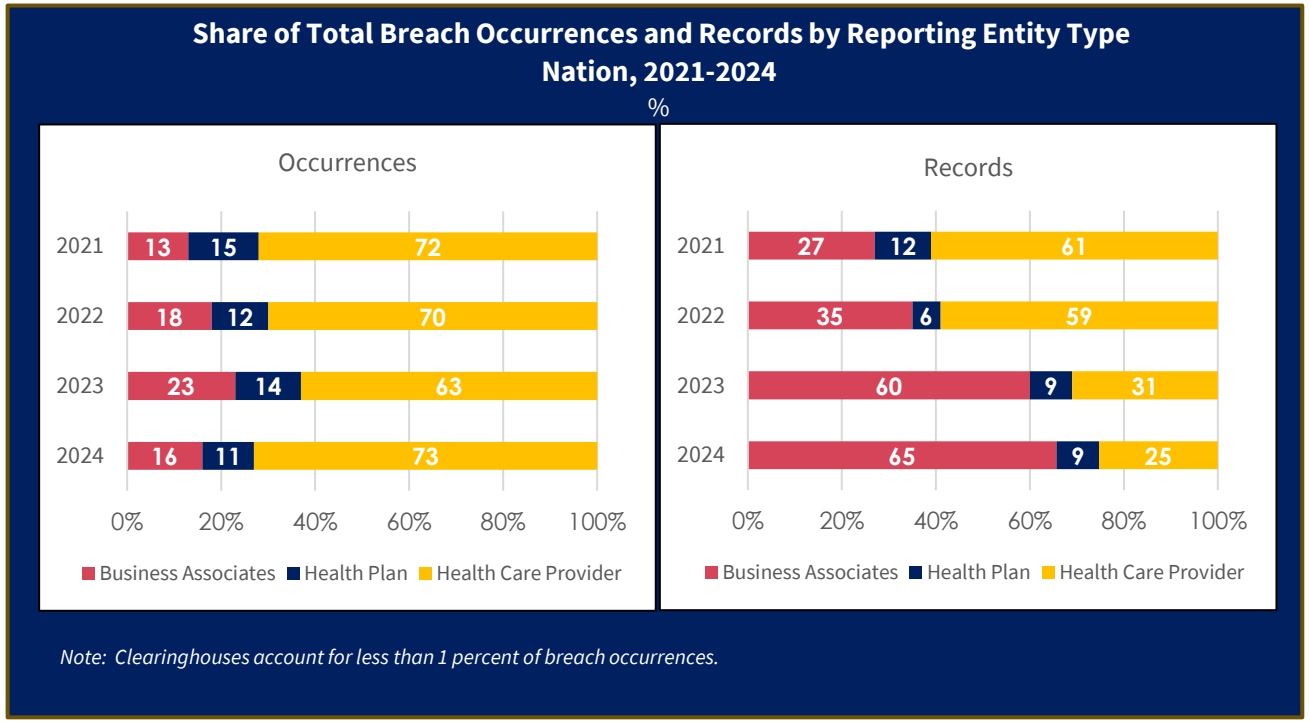
Breach Type

Table 3: Percent of Total Breach Occurrences and Records by Breach Type Nation, Maryland, & Cohort, 2021-2024									
Breach Type		Occurrences %				Records %			
		2021	2022	2023	2024	2021	2022	2023	2024
Nation	Hacking/IT	76	79	81	82	96	86	95	91
	Unauthorized Access/Disclosure	18	16	16	15	3	13	5	9
	Other*	5	5	3	3	1	1	<1	<1
Maryland	Hacking/IT	87	75	81	77	100	96	100	100
	Unauthorized Access/Disclosure	7	13	13	15	<1	1	<1	<1
	Other*	7	13	6	8	<1	3	<1	<1
Cohort	Hacking/IT	77	77	81	84	94	82	99	100
	Unauthorized Access/Disclosure	21	18	14	15	6	18	1	0
	Other*	2	4	5	1	<1	<1	<1	<1

*Notes: *Other includes breaches from improper disposal, loss, and theft.*
Percentages may not total 100 due to rounding.

- About four of five breaches reported in the nation, Maryland, and the cohort are the result of hacking/IT incidents involving technical intrusions of computer systems or networks
  - Accounts for the vast majority of records compromised
- Breaches involving unauthorized access/disclosures have experienced more growth in the last four years (see Appendix)
- Nationally, records have increased by 105 percent largely due to the Kaiser breach reported in 2024 (13.4M records)

Third-Party Breaches Have a Far-Reaching Impact



- The health care industry generally experiences more third-party breaches than other sectors
- Cybercriminals target third parties that provide a range of technology and services to support health care operations and the delivery of patient care
  - Unauthorized access through a third-party can potentially affect multiple organizations that rely on that vendor
- Records reported by BAs have nearly doubled since 2021 and account for more than half of all records in 2023 and 2024

Growing Cyber Risks

Geopolitical Forces and Tracking Technologies

- Nexus between cyberattacks and nation-state hackers acting on behalf of foreign governments (e.g., China, Russia, North Korea, and Iran)
  - Ransomware attacks targeting hospitals have increased by more than 300 percent, most of which are linked to Russia
  - A Russia-linked ransomware group (BlackCat/ALPHV) claimed responsibility for the Change Healthcare breach
- Risk of a breach increases if web browser tracking technologies are not carefully managed
  - Third-party online tracking codes (e.g., cookies and pixels) collect user information; misconfigurations can lead to over-sharing
  - A Kaiser breach inadvertently transmitted information on users' data with third parties (e.g., Google), such as name, IP address, and users' search activity (e.g., information about symptoms, drugs, injuries, and exercises)

MOVEit

- A third-party file transfer software exposed multiple organizations (worldwide) to a vulnerability in May 2023
  - Allowed CLOP, a Russian-linked ransomware group, to infect applications and steal data from MOVEit databases
- Across all industries, around 2,700 organizations were impacted by the MOVEit vulnerability
  - Estimated that one in five organizations were from the health care sector
- Welltok, a patient engagement software company, was the largest breach reported in 2023 (14.7M records)
- For Maryland, at least 6 of 16 breaches reported in 2023 (38 percent) and 2 of 13 in 2024 (14 percent) were linked to MOVEit
  - CMS reported two incidents involving BAs – Maximus in 2023 (2.3M records) and Wisconsin Physician Service Insurance Corporation in 2024 (3.1M records); makes up the majority of records (64 percent in 2023 and 82 percent in 2024)
  - Johns Hopkins, Westat, and Forward Healthcare also reported breaches

Change Healthcare

- Change Healthcare, a unit of UnitedHealth Group, experienced a breach involving a server not protected by multifactor authentication
  - The incident disrupted operations in revenue management (e.g., verifying eligibility and submitting claims) and patient care (e.g., delays in filling prescriptions)
- Largest number of records ever reported to OCR (190M)
  - Accounts for 68 percent of records nationally in 2024
- Considered the most significant and consequential cyberattack in the health care sector to date
  - Change Healthcare operates nationwide and connects with numerous provider and payer systems, processing about 15 billion health care transactions annually and about 73 percent of claims in Maryland

FTC Enforcement

Breaches Reported to the Federal Trade Commission and Penalties, 2023		
Company Name	**Company Type**	**Penalty Amount**
Monument	Addiction telehealth	$2.5 million
Better Help	Online mental health and counseling	$7.8 million
GoodRx	Telehealth and prescription drug discount platform	$1.5 million
Premom	Fertility tracking app	$200,000
Cerebral	Mental health telehealth	$7.1 million

- The FTC aims to protect the public from fraudulent, deceptive, and unfair practices; includes making sure companies take reasonable steps to protect PHI and do not mislead consumers about what is happening with their health information
- The FTC Health Breach Notification Rule applies to companies not regulated by HIPAA (e.g., health apps and fitness trackers)
- In 2023, the FTC took enforcement action against several digital health companies for impermissible disclosures of PHI to third parties

The End

Questions?

Appendix

Growth by Breach Type, 2021-2024

Table 4. CAGR by Breach Type, 2021-2024 %	Hacking/IT		Improper Disposal		Loss		Theft		Unauthorized Access/Disclosure	
	Occurrences	Records	Occurrences	Records	Occurrences	Records	Occurrences	Records	Occurrences	Records
Nation	3	43	-7	-62	-21	-37	-18	-10	-5	105
Maryland	-8	48					-100	-100	26	63
Cohort	-2	114			-100	-100	-21	64	-15	-35

Notes: Compound annual growth rate (CAGR) is a measure of growth for multiple time periods. CAGR cannot be calculated when the starting value is zero (i.e., zero breaches reported in 2021). A dash or (-) signifies a decrease.