MARYLAND Health Care Commission

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

Health Care Data Breaches

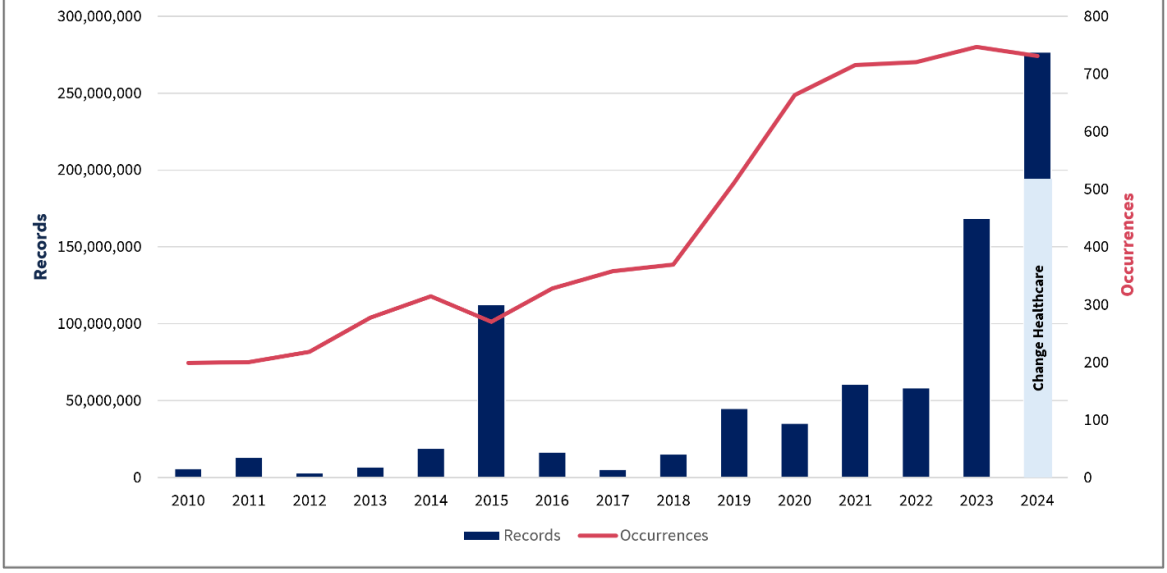
Impacts and Lessons Learned from Security Incidents in Maryland and the Nation

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.

The Health Information Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, requires covered entities (CE) and business associates (BA) to report all breaches[6] to the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR).[7, 8] OCR makes information on breaches affecting 500 individuals or more available in a public use file, which includes breach investigations that are active and closed.[9] 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.

ABOUT THIS SPOTLIGHT

The Maryland Health Care Commission conducted an analysis of breaches affecting 500 or more individuals from January 1, 2010 to December 31, 2024 using data downloaded from the OCR Breach Portal on March 11, 2025. The analysis centered on breach occurrences by state (i.e., the location of the reporting CE or BA) and a cohort of 11 states (Arizona, Maryland, Minnesota, Mississippi, New Hampshire, Nevada, Oklahoma, Texas, Virginia, Vermont, and Wisconsin). States within 10 percent of Maryland for hospital inpatient days per 100,000 population over three years (2020-2022) make up the cohort.[10] This spotlight highlights observations from the analysis with a focus on breaches reported to OCR from 2021 to 2024. Findings provide insights about cybersecurity, including common vulnerabilities, attack vectors, and approaches to strengthen breach preparedness, prevention, and response. For illustrative purposes, 2024 in Figure 1 (above) includes a count of records breached that was announced in January 2025 by Change Healthcare (or Change), a subsidiary of UnitedHealth Group (acquired in 2022); this updates the record count that Change previously reported to OCR in October 2024 (from 100 million to 190 million records). The remaining analysis included herein only includes 100 million records for Change, since the additional records were not in the breach data obtained from OCR as of March 11, 2025.

Table 1. Cohort Quartile Ranking, Breaches Per 100,000, and Other Demographics

Quartile (Highest to Lowest) **Breach Occurrences 2021-2024**	**Cohort (Total Breaches 2021-2024)**	**Population (2024)**	**Occurrences per 100,000** 2021-2024	**Physicians** Total / per 100,000	**Hospitals** Total / per 100,000
Quartile 4	**TX (174)**	31,290,831	0.55	0.24	1.63
	AZ (46)	7,582,384	0.61	0.26	1.15
Quartile 3	**VA (39)**	8,811,195	0.44	0.31	1.07
	MN (39)	5,793,151	0.67	0.34	2.14
	MD (36)	6,263,220	0.57	0.44	0.75
Quartile 2	**WI (34)**	5,960,975	0.57	0.33	2.23
	OK (27)	4,095,393	0.66	0.25	3.05
	NH (22)	1,409,032	1.56	0.32	1.99
Quartile 1	**MS (21)**	2,943,045	0.71	0.25	3.36
	NV (17)	3,267,467	0.52	0.20	1.41
	VT (5)	648,493	0.77	0.42	2.16

Notes: Population data was obtained from the US Census Bureau; data on physicians is as of January 2025 and hospitals is as of January 2022 and was obtained from Kaiser Family Foundation; quartile ranking for the cohort is based on total breach occurrences from 2021-2024 and is ordered from the highest to lowest number of breaches by state; quartile ranking divides a dataset into four equal groups (quartiles) based on their relative position to the mean.

SUMMARY

Records Compromised are Increasing from Far-Reaching Third-Party Breaches

Health care organizations implement and maintain cybersecurity measures to protect the interconnected systems that collect, store, and share protected health information (PHI). Cybersecurity reduces the risk of a breach; however, cybercriminals still find new ways to exploit vulnerabilities. Over the last four years, growth in breach occurrences has remained relatively flat, but the number of records has increased substantially (Table 2). Millions of records can be compromised by a single breach. Third parties often maintain or have access to large repositories of data, making them prime targets for cybercriminals.[11] In February 2024, hackers[12] breached Change Healthcare, a health care payment processing company (i.e., clearinghouse) that supports billing and insurance for many provider organizations, including hospitals, medical offices, and pharmacies. The security incident caused disruptions in revenue management (e.g., verifying eligibility and submitting claims) and patient care (e.g., delays in filling prescriptions).[13] The incident is still under investigation and considered the most significant and consequential cyberattack in the health care sector to date.[14] Notably, the health care industry experiences more third-party breaches than other sectors.[15]

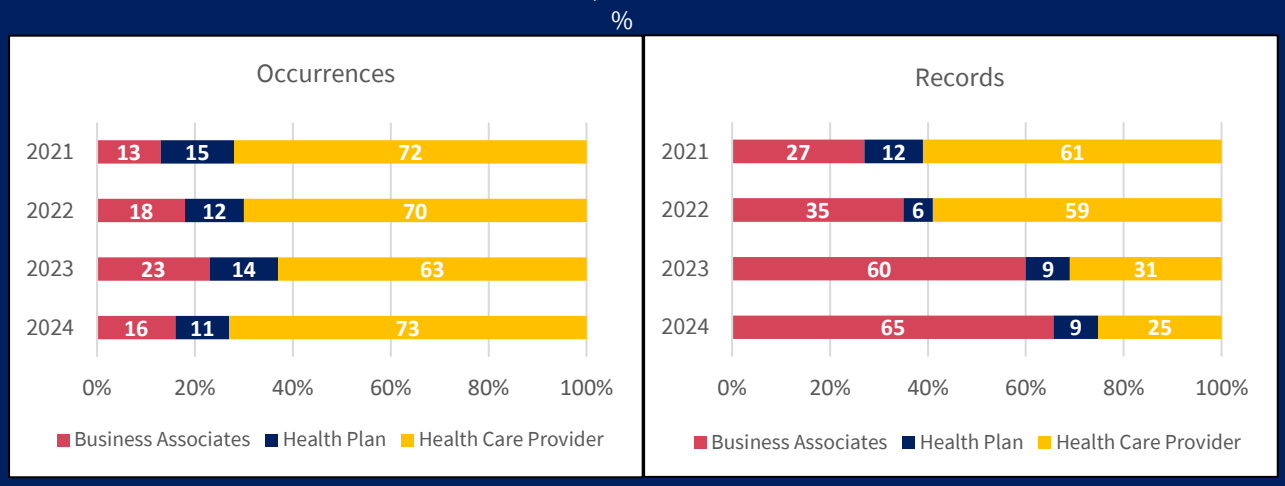
Table 2. Overall Snapshot of Breaches, 2021-2024

	Occurrences #					Records #				
	2021	2022	2023	2024	CAGR %	2021	2022	2023	2024	CAGR %
Nation All states	715	720	747	731	1	60,813,579	58,443,868	168,666,266	186,719,066	45
Maryland	15	16	16	13	-5	1,180,040	217,660	3,676,102	3,802,477	48
Cohort 11 states	171	157	155	148	-5	13,620,219	17,310,973	36,396,603	125,507,828	110

Note: The cohort includes records (100 million) reported by Change in Minnesota (where United Health Group is headquartered). Compound annual growth rate (CAGR) is a measure of growth for multiple time periods. A dash or (-) signifies a decrease.

The use of third parties is mission critical to support health care operations and the delivery of patient care. Provider organizations depend on a variety of vendors for a wide range of technology and services, making third-party risk management an integral component of data security. When a cyberattack occurs at a BA – or third parties that support a BA – its customers become collateral damage. Unauthorized access through a third-party provides a digital pathway to potentially affect multiple organizations that rely on that vendor[16] (e.g., Change operates nationwide and connects with numerous provider and payer systems, processing about 15 billion health care transactions annually).[17, 18] While cybercriminals increasingly target third parties, providers still account for the largest share of breach occurrences. However, providers are reporting fewer records each year; from 2021 to 2024, records decreased from 61 percent to 24 percent. Records reported by BAs have nearly doubled over that time, accounting for more than half of all records compromised in 2023 and 2024 (Figure 2/Appendix B).

Figure 2: Share of Total Breach Occurrences and Records by Reporting Entity Type Nation, 2021-2024



Note: Clearinghouses account for less than 1 percent of breach occurrences.

Reporting Entities Do Not Entirely Reflect Where Security Failures Occur

HIPAA requires a BA to notify the applicable CE when a breach occurs at or by the BA.[19] CEs are responsible for notifying individuals whose records were compromised and may delegate this responsibility to the BA[20] (e.g., Change was instructed to send out breach notifications to providers and payers; letters were mailed to impacted individuals beginning in June 2024).[21] Breaches may be reported to OCR by a BA, CE, or a combination of the two. In 2023, Johns Hopkins[22] was one of many entities that fell victim to the MOVEit data breach, a ransomware attack that impacted a wide range of organizations in the public and private sectors. MOVEit is a file transfer program owned by Progress Software, a Massachusetts-based technology company. Johns Hopkins reported a breach of more than 300,000 records to OCR.[23] Virginia-based Maximus, a BA with federal, state, and local government contracts, also reported a breach of 9.2 million records stemming from MOVEit.[24] Several Maximus clients opted to individually report the breach, including the Virginia Department of Medical Assistance Services (1.7 million records)[25] and the Centers for Medicare and Medicaid Services (CMS) (2.3 million records). In 2024, CMS reported a second breach (3.1 million records) due to another BA also affected by MOVEit, Wisconsin Physician Service Insurance Corporation.[26] Third party breaches reported by CMS account for nearly all records compromised by health plans in Maryland for 2023 and 2024 (Appendix B), yielding a smaller share of records among BAs compared to the cohort and the nation (Table 3). Within the cohort, a Nevada-based medical transcription company, Perry Johnson & Associates (PJ&A), experienced a cyberattack in 2023. PJ&A reported a breach of 9.3 million records as a BA to OCR; several CEs impacted chose to file separately with OCR, including a Texas-based urgent care and occupational health provider, Concentra (4 million records). [27]

Table 3: Percentage of Total Breach Occurrences and Records by Reporting Entity Type Nation, Maryland, & Cohort, 2021-2024									
Reporting Entity Type		Occurrences %				Records %			
		2021	2022	2023	2024	2021	2022	2023	2024
Nation	Business Associate	13	18	23	16	27	35	60	65
	Health Plan	15	12	14	11	12	6	9	9
	Health Care Provider	72	70	63	73	61	59	31	25
Maryland	Business Associate	13	31	31	31	5	52	11	12
	Health Plan	7	19	19	8	<1	14	64	82
	Health Care Provider	80	50	50	62	95	35	25	6
Cohort	Business Associate	13	22	18	16	28	31	70	85
	Health Plan	11	10	12	6	1	5	12	3
	Health Care Provider	75	68	70	78	71	65	18	12

Notes: Breaches reported by health care clearinghouses are not represented in the table above; health care clearinghouses did not report breaches in 2022 and represent <1 percent of occurrences and records nationally in 2021, 2022, and 2023.
One breach (10,000 records) was reported in 2023 that did not specify reporting entity type.
Percentages may not total 100 due to rounding.

A Closer Look at Breaches Involving Change and MOVEit

Change Healthcare

The cyberattack on Change, a unit of UnitedHealth Group, occurred after ransomware (a type of malicious software or malware) compromised a server not protected by multifactor authentication, an industry security standard requiring two or more steps to log into a system (e.g., code or fingerprint).[28] Upon discovery in February 2024, Change disconnected its systems to stem the ransomware's spread. The event disrupted operations for a large majority of payers and providers across the nation. Hospitals reported impacts to patient care (74 percent) and financial viability (94 percent).[29] A Russia-linked ransomware group – BlackCat/ALPHV – claimed responsibility and demanded money to return services online.[30] Change reportedly paid a ransom of approximately $22 million (350 bitcoins).[31] Paying a ransom does not alleviate total costs related to response, system reconstitution, or business losses.[32] The breach is estimated to cost UnitedHealth Group in excess of $2 billion.[33] In July 2024, Change filed a preliminary breach report with OCR as a BA, noting 500 individual records affected. The records count has since been updated twice to 100 million records in October 2024 and 190 million records in January 2025. Change processes about half of all medical claims in the U.S.[34] and about 73 percent of claims in Maryland.[35]

MoveIt

A vulnerability in the software solution MOVEit was exploited by CLOP, a Russian-linked ransomware group with a history of targeting health care entities and file transfer solutions.[36] The incident began on May 27, 2023 and allowed CLOP to gain unauthorized access to thousands of organizations worldwide that rely on MOVEit for secure file transfers.[37] A warning was issued on May 30, 2023, and a patch to repair the vulnerability was made available the next day.[38] Welltok, a patient engagement software company, had more than 14.7 million records affected by MOVEit, making it the largest breach reported to OCR in 2023. Across all industries, around 2,700 organizations were impacted by the MOVEit vulnerability; it is estimated that one in five organizations were from the health care sector.[39] In Maryland, at least 6 of 16 breaches reported in 2023 (38 percent) and 2 of 13 in 2024 (14 percent) noted the cause was related to MOVEit.[40] Prior to MOVEit, CLOP claimed responsibility for exploiting a vulnerability in a different secure file transfer solution offered by Fortra GoAnywhere (January 2023). The incident affected 130 organizations across all industries of which many were in the health care sector, including Tennessee-based provider Community Health Systems (962,884 records) and a Florida-based BA, NationBenefits, LLC (3,037,303 records).[41, 42]

Cyber Risk is Influenced by Geopolitical Forces

There is a growing nexus between cyberattacks and nation-state hackers acting on behalf of foreign governments (e.g., China, Russia, North Korea, and Iran).[43] Nation-state hackers seek to disrupt critical infrastructure and gather intelligence from patient records stored in various platforms, including electronic medical records and genomic databases.[44] Ransomware attacks are common and growing; attacks targeting hospitals have increased by more than 300 percent, most of which are linked to Russia.[45] Ransomware is a more pronounced issue in health care because organizations are more willing to pay money (up to millions of dollars) to minimize disruption in accessing data necessary to provide care.[46] Such disruption impacts health care operations, putting patient safety at risk. Hospitals rely on public-private partnerships and other collaborative efforts (e.g., American Hospital Association, Healthcare-Information Sharing and Analysis Center, and HHS-sponsored Health Care Industry Cyber Security Task Force) to help prepare for and respond to cyberattacks.[47] Hacking/IT incidents involving technical intrusions of computer systems or networks account for the vast majority of records compromised (Table 4/Appendix C) with about four of five breaches reported as the result of such incidents (Table 5/Appendix D). Notably, a large majority of cyber criminals operate on behalf of an adversarial nation state that does not cooperate with or extradite these criminals to the United States.[48]

Table 4: 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.

Unintentional Human Factors Cause More Breaches

Preventing data breaches requires a combination of people, processes, and technology. Technical safeguards required by the HIPAA security rule and ongoing security awareness and training strengthen risk management practices to help mitigate risks caused by human error.[49] By and large, more breaches are caused by unintentional human factors (e.g., falling for deceptive emails, opening infected files, misconfiguring security settings, and sending sensitive information to the wrong recipients) than malicious intent.[50] Unauthorized access/disclosure[51] is the second most common breach type (after hacking/IT). Growth in unauthorized access/disclosure breaches has generally declined, except for in Maryland (Table 5), where health care providers, a health plan, and BAs reported breaches from 2021 through 2024. The largest of these unauthorized access/disclosures was reported by a health plan (CMS) in 2023 (10,011 records). Nationally, records from unauthorized access/disclosures have increased significantly (105 percent), largely due to a breach reported by a health plan, Kaiser Foundation Health Plan Inc. (13.4 million records) in 2024.

Table 5. 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.

Unauthorized access/disclosure can occur if web browser tracking technologies are not carefully managed. Third-party online tracking codes (e.g., pixels)[52] collect user information, and misconfigurations can lead to over-sharing.[53] Kaiser's use of tracking codes inadvertently transmitted information on patients' data and browsing behavior with third parties, such as Microsoft (Bing), Google, and X (Twitter). The information included names, IP addresses, sign-in statuses, and user activity (e.g., searching for information about symptoms, drugs, injuries, and exercises).[54] The Kaiser breach accounts for 88 percent of records nationally from unauthorized disclosures in 2024 (Appendix C), making it the largest confirmed health care data breach involving online tracking codes reported to OCR to date.[55] Kaiser is among other health care organizations (Monument, Tempest, and Cerebral) that had used online tracking codes to collect and disclose user analytics to third parties.[56] Generally, CEs and BAs can use services that track and analyze online user behavior for general information web pages, but this is not permitted for web pages that require a user login (e.g., patient portal) without a Business Associate Agreement (BAA) in place (some of the most commonly used services, like Google Analytics and Meta's Pixel, do not offer BAAs).[57, 58] HHS has issued multiple guidance documents throughout 2022-2024 around the use of these tracking codes by HIPAA-regulated entities, including examples of when the codes can and cannot be used.[59, 60]

Beyond HIPAA

In addition to the federal floor for privacy and security established by HIPAA, the Federal Trade Commission (FTC) Act[61] also applies to HIPAA-regulated entities and other companies[62] that collect, use, and share consumers' PHI. The Act aims to protect the public from fraudulent, deceptive, and unfair practices in or affecting commerce; this 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 that are not HIPAA CEs or BAs. These companies are required to provide notice to affected consumers, the FTC, and in some cases the media when they experience a breach of unsecured PHI.[63] In 2023, the FTC took enforcement action for the first time; this included GoodRx for failure to notify consumers that it had shared user health data with third parties to target them with health-related advertisements.[64] Other enforcement actions have been take by the FTC against several other companies for impermissible disclosures of PHI to third parties like Google and Facebook (Table 6).[65]

Table 6: 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

CONCLUSION

The growing and persistent threat of cyberattacks against the health care sector highlights the critical need for adaptive and robust cybersecurity strategies to safeguard patient privacy and operational integrity. While zero trust and other security measures strengthen defenses, they are not foolproof, as evidenced by the increasing frequency of breaches across the health care ecosystem and supply chain. In general, HIPAA and state-level policies have not evolved as fast as cybercrime. In December 2024, HHS issued a Notice of Proposed Rulemaking[66] to update the HIPAA Security Rule with stronger cybersecurity measures designed to improve protections for electronic PHI. Efforts to bolster cybersecurity in health care must continue to evolve to improve security practices in ways that support incident preparedness and response.

LIMITATIONS

Breaches are reported for the state where the entity is headquartered, even if the entity operates in multiple states. Breach year reflects when the breach was reported to OCR, which may be different from the year in which the incident occurred.[67] A single security incident can lead to multiple breaches reported to OCR (e.g., MOVEit). Breach data does not reflect whether a BA is reporting on behalf of multiple clients (e.g., Change). Specific information related to origin of the breach, cause, and type of patient information compromised is not available for all breach reports.

APPENDIX A

Health Care Data Breaches 2010-2024, Nation		
Year	**Occurrences**	**Records**
2024	731	186,719,066 276,719,066
2023	747	168,666,266
2022	720	58,433,868
2021	715	60,813,579
2020	663	35,309,732
2019	511	44,969,724
2018	369	15,236,139
2017	358	5,314,987
2016	328	16,711,004
2015	270	112,466,720
2014	314	19,073,551
2013	277	7,018,839
2012	218	2,854,525
2011	200	13,162,158
2010	199	5,932,276
Total	**6,638**	**752,847,303**

Note: For 2024, the record count in gray reflects an updated number announced by Change Healthcare in January 2025 (from 100 million to 190 million records); this updated number of records was not in the breach data obtained from OCR as of March 11, 2025.

APPENDIX B

Breach Occurrences and Records by Covered Entity Type, 2021-2024									
Reporting Entity Type		**Occurrences**				**Records**			
		2021	**2022**	**2023**	**2024**	**2021**	**2022**	**2023**	**2024**
Nation	Business Associate	93	129	173	115	16,208,296	20,537,299	101,262,988	121,942,869
	Health Plan	104	87	103	78	7,204,480	3,294,517	15,758,468	17,684,871
	Health Care Provider	516	504	468	535	37,382,903	34,612,052	51,631,735	46,787,070
	Health Care Clearinghouse	2	0	2	3	17,900	0	3,075	304,256
	Total	**715**	**720**	**747**	**731**	**60,813,579**	**58,443,868**	**168,666,266**	**186,719,066**
Maryland	Business Associate	2	5	5	4	54,825	112,734	409,445	465,402
	Health Plan	1	3	3	1	2,693	29,702	2,353,052	3,112,815
	Health Care Provider	12	8	8	8	1,122,522	75,224	913,605	224,260
	Health Care Clearinghouse	0	0	0	0	0	0	0	0
	Total	**15**	**16**	**16**	**13**	**1,180,040**	**217,660**	**3,676,102**	**3,802,477**
Cohort	Business Associate	22	35	28	24	3,751,787	5,286,736	25,633,405	106,574,859
	Health Plan	19	15	19	9	174,674	834,571	4,197,634	3,704,644
	Health Care Provider	129	107	108	115	9,691,796	11,189,666	6,565,564	15,228,325
	Health Care Clearinghouse	1	0	0	0	1,962	0	0	0
	Total	**171**	**157**	**155**	**148**	**13,620,219**	**17,310,973**	**36,396,366**	**125,507,828**

Note: One breach (10,000 records) was reported in 2023 that did not specify reporting entity type.

APPENDIX C

Breach Occurrences and Records by Breach Type, 2021-2024									
Breach Type		**Occurrences**				**Records**			
		2021	**2022**	**2023**	**2024**	**2021**	**2022**	**2023**	**2024**
Nation	Hacking/IT	546	570	606	596	58,599,603	50,544,828	160,153,675	170,523,502
	Improper Disposal	5	4	5	4	190,508	8,191	12,360	10,309
	Loss	10	11	4	5	33,358	17,665	38,928	8,501
	Theft	24	20	12	13	107,958	380,500	29,045	77,833
	Unauthorized Access/Disclosure	130	115	120	113	1,882,152	7,492,684	8,432,258	16,098,921
	Total	715	720	747	731	60,813,579	58,443,868	168,666,266	186,719,066
Maryland	Hacking/IT	13	12	13	10	1,175,982	209,213	3,660,955	3,791,025
	Improper Disposal	0	0	0	1	0	0	0	568
	Loss	0	1	0	0	0	897	0	0
	Theft	1	1	1	0	1,553	6,190	4,000	0
	Unauthorized Access/Disclosure	1	2	2	2	2,505	1,360	11,147	10,884
	Total	15	16	16	13	1,180,040	217,660	3,676,102	3,802,477
Cohort	Hacking/IT	131	121	126	124	12,806,395	14,170,946	36,188,681	125,255,455
	Improper Disposal	0	0	2	1	0	0	3,222	568
	Loss	2	4	1	0	2,446	7,189	13,184	0
	Theft	2	3	4	1	7,687	52,779	8,644	34,063
	Unauthorized Access/Disclosure	36	29	22	22	803,691	3,080,059	182,872	217,742
	Total	171	157	155	148	13,620,219	17,310,973	36,396,603	125,507,828

APPENDIX D

Occurrences and Records by Breach Type Hacking/IT (Hacking) and Unauthorized Access Disclosure (UAD) Cohort, 2021-2022										
State	Population	Breach type	Occurrences				Records			
			2021	2022	2023	2024	2021	2022	2023	2024
TX	31,290,831	Hacking	35	44	48	48	5,511,575	6,900,448	5,936,597	11,269,155
		UAD	20	8	6	11	586,465	28,552	15,176	136,050
		Other	0	1	4	0	0	1,009	17,003	0
VA	8,811,195	Hacking	13	16	11	9	272,026	76,277	11,746,161	256,863
		UAD	2	6	3	1	5,717	11,281	2,421	1,074
		Other	0	2	0	0	0	5,091	0	0
AZ	7,582,384	Hacking	13	12	12	13	1,017,881	1,598,258	775,040	4,065,886
		UAD	1	4	4	3	1,866	3,075	11,706	15,811
		Other*	1	0	1	0	717	0	1,034	0
MD	6,263,220	Hacking	13	12	13	10	1,175,982	209,213	3,660,955	3,791,025
		UAD	1	2	2	2	2,505	1,360	11,147	10,884
		Other*	1	2	1	1	1,553	7,087	4,000	568
WI	5,960,975	Hacking	13	10	10	10	2,547,882	4,500,850	571,391	813,754
		UAD	3	4	1	0	3,667	3,021,972	134,000	0
		Other*	1	1	0	0	1,729	45,580	0	0
MN	5,793,151	Hacking	12	5	14	11	376,409	104,532	3,447,251	101,041,667
		UAD	6	1	4	1	10,380	1,584	7,125	715
		Other*	0	0	0	0	0	0	0	0
OK	4,095,393	Hacking	8	8	5	8	249,638	467,592	69,354	3,316,872
		UAD	1	1	0	1	1,038	8,629	0	38,945
		Other*	1	0	1	0	6,134	0	3,013	0
NV	3,267,467	Hacking	8	3	2	3	1,473,413	29,422	9,307,210	19,852
		UAD	1	1	0	1	1,833	1,861	0	1,017
		Other*	0	0	0	1	0	0	0	34,063
MS	2,943,045	Hacking	8	2	9	5	100,574	22,059	651,532	424,550
		UAD	0	1	1	0	0	1,059	777	0
		Other*	0	0	0	0	0	0	0	0
NH	1,409,032	Hacking	5	7	2	6	56,904	173,022	23,190	255,831
		UAD	1	0	0	2	190,220	0	0	13,246
		Other*	0	1	0	0	0	1,201	0	0
VT	648,493	Hacking	3	2	0	0	24,111	89,273	0	0
		UAD	0	1	1	0	0	686	520	0
		Other*	0	0	0	0	0	0	0	0

*Note: *Other includes breaches from improper disposal, loss, and theft*

ENDNOTES

[1] Ransomware is a type of malicious software that blocks access to computer systems until a sum of money is paid.
[2] Harvard Business Review, *Preventing the Next Big Cyberattack on U.S. Health Care,* May 2024. Available at: hbr.org/2024/05/preventing-the-next-big-cyberattack-on-u-s-health-care.
[3] A zero trust approach ensures continuous monitoring by verifying the authenticity and privileges of devices and users, no matter where they are in the network (i.e., never trust, always verify). More information is available at: www.weforum.org/stories/2023/05/cyber-attacks-on-healthcare-rise-zero-trust.
[4] Okta, *The State of Zero Trust Security in Global Organizations,* 2020. Available at: www.okta.com/resources/reports/state-of-zero-trust-security-in-global-organizations/.
[5] Average number of breaches daily was calculated by dividing the total breach occurrences from January 1, 2018-December 31, 2024 (4,426) and the number of days during that time period (2,556).
[6]OCR defines a HIPAA breach as an impermissible use or disclosure of protected health information (PHI) under the Privacy Rule that compromises the security or privacy of that information.
[7] U.S. Department of Health and Human Services, *Submitting Notice of a Breach to the Secretary*. Available at: www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html.
[8] § 164.402 of the HIPAA Breach Notification Rule: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D/section-164.402.
[9] The OCR Breach Portal is available at: ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
[10] Information on inpatient days was obtained from the 2022 American Hospital Association Annual Survey, which uses a consistent definition and reporting methodology. Data was accessed from the Kaiser Family Foundation: www.kff.org/statedata/.
[11] Modern Healthcare, *Finding Some Good News after a Bad Year for Cyberattacks*, January 2025. Available at: www.modernhealthcare.com/cybersecurity/healthcare-data-breaches-2024-hhs.
[12] The breach was linked to a Russian ransomware group ALPHV BlackCat.
[13] Cybersecurity Dive, *Change Healthcare Cyberattack Having 'Far-Reaching' Effects on Providers,* March 2024. Available at: www.cybersecuritydive.com/news/change-healthcare-providers-impact/709236/.
[14] American Hospital Association, *Third-Party Cyber Risk Impacts the Health Care Sector the Most. Here's How to Prepare*, August 2024. Available at: www.aha.org/news/aha-cyber-intel/2024-08-05-third-party-cyber-risk-impacts-health-care-sector-most-heres-how-prepare.
[15] The HIPAA Journal, *Healthcare Experiences More Third-Party Data Breaches Than Any Other Sector*, March 2024. Available at: www.hipaajournal.com/healthcare-highest-third-party-breaches/.
[16] See n. 14, *Supra*.
[17] Chief Healthcare Executive, *Cybersecurity and Hospitals: Big Risks Come from Third Parties,* March 2024. Available at: www.chiefhealthcareexecutive.com/view/cybersecurity-and-hospitals-big-risks-come-from-third-parties.
[18] Change Healthcare reported the breach as a BA because while it acts as a clearinghouse, it also performs services for CEs that involve the disclosure of PHI, making it a BA under HIPAA regulations.
[19] The notification must be made without unreasonable delay and no later than 60 days from discovery of the breach. More information is available at: www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.
[20] This depends on various circumstances, such as the functions the BA performs on behalf of the CE and which entity has the relationship with the individual.
[21] Change Healthcare, *HIPAA Website Substitute Notice*. Available at: www.changehealthcare.com/hipaa-substitute-notice.html
[22] Three Johns Hopkins organizations reported breaches from the MOVEit incident: Howard County General Hospital (provider - 2,75 records), Johns Hopkins Medicine (provider - 310,405 records), and Johns Hopkins Health System Corporation (business associate - 2,584 records).
[23] Johns Hopkins Medicine, *Data Attack*. Available at: www.hopkinsmedicine.org/data-attack.
[24] Healthcare Finance News, *CMS, Maximus Investigating Data Breach Involving Personal Health Information*, August, 2023. Available at: www.healthcarefinancenews.com/news/cms-maximus-investigating-data-breach-involving-personal-health-information.
[25] The HIPAA Journal, *Security Breaches in Healthcare in 2023*, January 2024. Available at: www.hipaajournal.com/wp-content/uploads/2024/01/Security_Breaches_In_Healthcare_in_2023_by_The_HIPAA_Journal.pdf.
[26] The HIPAA Journal, *CMS Confirms 3.1 Million Individuals Affected by MOVEit Hack on Wisconsin Physicians Service*, September 2024. Available at: www.hipaajournal.com/cms-wisconsin-physicians-service-moveit-hack/.
[27] The HIPAA Journal, *Concentra Confirms Almost 4 Million Patients Affected by PJ&A Data Breach*, January 2024. Available at: www.hipaajournal.com/pja-data-breach/.
[28] House Committee on Energy & Commerce, *What We Learned: Change Healthcare Cyber Attack*, May 2024. Available at: energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack.
[29] American Hospital Association, *AHA Survey: Change Healthcare Cyberattack Significantly Disrupts Patient Care, Hospitals' Finances*, March 2024. Available at: www.aha.org/2024-03-15-aha-survey-change-healthcare-cyberattack-significantly-disrupts-patient-care-hospitals-finances.

[30] Congress.gov, *The Change Healthcare Cyberattack and Response Considerations for Policymakers*, April 2024. Available at: crsreports.congress.gov/product/pdf/IN/IN12330.
[31] I*bid.*
[32] *Ibid.*
[33] Bank Info Security, *Change Healthcare Attack Cost Estimate Reaches Nearly $2.9B*, October 2024. Available at: www.bankinfosecurity.com/change-healthcare-attack-cost-estimate-reaches-nearly-29b-a-26541.
[34] Journal of AHIMA, *Revenue Cycle Leaders Share Impact, Insights from Change Healthcare Cyberattack*, December 2024. Available at: journal.ahima.org/page/revenue-cycle-leaders-share-impact-insights-from-change-healthcare-cyberattack#:~:text=As%20the%20nation's%20largest%20electronic,associated%20payer%20payments%20to%20providers.
[35] Percentage calculated based on data obtained through MHCC's 2023 EDI Progress Report. COMAR 10.25.09, Requirements for Payers to Designate Electronic Health Networks requires payers with premiums of $1 million or more to annually report census-level data on electronic health care transactions.
[36] HHS Office of Information Security, *Clop Allegedly Targets Healthcare Industry in Data Breach*, February 2023. Available at: www.hhs.gov/sites/default/files/clop-allegedly-targeting-healthcare-industry-sector-alert.pdf.
[37] Data breaches resulting from the MOVEit vulnerability affected more than 2,300 organizations across sectors as of January 2024, with around 20 percent of occurring within the health care sector. More information is available at: www.cybersecuritydive.com/news/progress-software-moveit-meltdown/703659/#:~:text=Clop%2C%20a%20highly%20prolific%2C%20financially,from%20the%20file%2Dtransfer%20service
[38] Reuters, *MOVEit Hack Spawned over 600 Breaches but is Not Done Yet - Cyber Analysts*, August 2023. Available at: www.reuters.com/technology/moveit-hack-spawned-around-600-breaches-isnt-done-yet-cyber-analysts-2023-08-08/.
[39] Cybersecurity Dive, *Progress Software's MOVEit Meltdown: Uncovering the Fallout*, January 2024. Available at: www.cybersecuritydive.com/news/progress-software-moveit-meltdown/703659/.
[40] Organizations include CMS, three Johns Hopkins entities (Johns Hopkins Health System Corporation, Howard County General Hospital, and Johns Hopkins Medicine), Forward Healthcare, and Westat.
[41] File transfer services are used to securely share and synchronize files across systems. Progress Software's MOVEit, Fortra's GoAnywhere and IBM Aspera Faspex were hit by supply-chain attacks in 2023. More information is available at: www.cybersecuritydive.com/news/progress-software-moveit-meltdown/703659/
[42]HHS Office of Information Security, *Clop Allegedly Targets Healthcare Industry in Data Breach*, February 2023. Available at: www.hhs.gov/sites/default/files/clop-allegedly-targeting-healthcare-industry-sector-alert.pdf.
[43] The HIPAA Journal, *US Calls for Russia and Other States to Take Action Over Healthcare Ransomware Attacks*, November 2023. Available at: https://www.hipaajournal.com/us-russia-action-healthcare-ransomware-attacks/.
[44]Leech | Tishman, *Hacking and Healing: Nation-States, Cyber Attacks, and Healthcare Law*, April 2024. Available at: https://www.leechtishman.com/insights/blog/hacking-and-healing-nation-states-cyber-attacks-and-healthcare-law/ .
[45] Becker's Health IT, *Russian Hackers Targeting Healthcare*, May 2024. Available at: www.beckershospitalreview.com/cybersecurity/russian-hackers-targeting-healthcare.html.
[46] Microsoft, *US Healthcare at Risk: Strengthening Resiliency Against Ransomware Attacks*, https://www.microsoft.com/en-us/security/security-insider/emerging-threats/US-healthcare-at-risk-strengthening-resiliency-against-ransomware-attacks#Chapter-One-article.
[47] AHA Center for Health Innovation, *Ransomware Attacks on Hospitals Have Changed*. Available at: www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed.
[48] *Ibid.*
[49] Chukwudi Tabitha Aghaunor, Patience Eshua, Tawo Obah and Oluwatoyin Aromokeye. *Data security strategies to avoid data breaches in modern information systems*. World Journal of Advanced Research and Reviews, 2025, 25(01), 827-849. Article DOI: doi.org/10.30574/wjarr.2025.25.1.3906.
[50] Yeo LH, Banfield J. Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. Perspect Health Inf Manag. 2022 Mar 15;19(Spring):1i. PMID: 35692854; PMCID: PMC9123525
[51] Breaches reported as unauthorized access and disclosure encompass incidents that do not fall under the other breach type categories (i.e., hacking/IT, loss, theft, and improper disposal). This category is broad and covers a wide range of security incidents such as accidentally emailing or mailing PHI to the wrong recipient, employee snooping, coding mistakes that expose PHI, unauthorized use of PHI for marketing, etc.
[52] Tracking technologies are used to gather information about users or their actions as they interact with a website or mobile app. More information about tracking technologies and HIPAA is available at: www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.
[53] Reflectiz, *Online Tracking in Healthcare: How to Combat Critical Privacy Dangers, June 2024.* Available at: www.reflectiz.com/blog/online-tracking-healthcare/.
[54] Fierce Healthcare, *Kaiser Permanente Reports Data Breach Impacting 13.4M Health Plan Members*, April 2025. Available at: www.fiercehealthcare.com/providers/kaiser-permanente-says-134m-impacted-data-breach.
[55] The HIPAA Journal, *Kaiser Permanente Website Tracker Breach Affects 13.4 Million Individuals*, April 2024. Available at: www.hipaajournal.com/kaiser-permanente-website-tracker-breach-affects-13-4-million-individuals/.
[56] HIT Consultant. *What All Healthcare IT Leaders Must Understand About the Kaiser Permanente Breach*, December 2024. Available at: hitconsultant.net/2024/12/03/what-all-healthcare-it-leaders-must-understand-about-the-kaiser-permanente-breach/.

[57] The HIPAA Journal, *Is Google Analytics HIPAA Compliant?* December 2023. Available at: www.hipaajournal.com/is-google-analytics-hipaa-compliant/.
[58] Many websites mobile applications utilize more than 30 third-party scripts to enable key functionalities. More information is available at: hitconsultant.net/2024/12/03/what-all-healthcare-it-leaders-must-understand-about-the-kaiser-permanente-breach/.
[59] Inside Privacy, *HHS OCR Updates Tracking Technologies Guidance,* March 2024. Available at: www.insideprivacy.com/health-privacy/hhs-ocr-updates-tracking-technologies-guidance/.
[60] HHS guidance for HIPAA regulated entities around tracking technologies is available at: www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.
[61] The Federal Trade Commission (FTC) was created on September 26, 1914 when President Woodrow Wilson signed the Federal Trade Commission Act into law. More information is available at: www.ftc.gov.
[62] Includes entities offering technology and services, such as mobile health applications, personal health devices, and genetic information services and products.
[63] More information about Complying with FTC's Health Breach Notification Rule is available at: www.ftc.gov/business-guidance/resources/complying-ftcs-health-breach-notification-rule-0.
[64] FTC, *FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising*, February 2023. Available at: www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising.
[65] The HIPAA Journal, *Healthcare Data Breach Statistics,* March 2025. Available at: www.hipaajournal.com/healthcare-data-breach-statistics/.
[66]U.S. Department of Health and Human Services, *HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information*, December 27, 2024. Available at: www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html.
[67] In some cases, there is a delay in discovery of a breach. Organizations are required to report the breach to OCR within 60 calendar days of discovery.