Health Care Data Breaches:

An Assessment of Breach Trends in Maryland and the Nation

2010 – 2019

January 2020

Andrew N. Pollak, MD
CHAIRMAN

Ben Steffen
EXECUTIVE DIRECTOR

MARYLAND HEALTH CARE COMMISSION

Andrew N. Pollak, MD, Chairman
Professor and Chair, Department of Orthopaedics
University of Maryland School of Medicine
Chief of Orthopaedics, University of Maryland Medical System

Cassandra Boyer
Business Operations Manager
Enterprise Information Systems Directorate
US Army Communications Electronics Command

Marcia Boyle
Founder
Immune Deficiency Foundation

Martin L. "Chip" Doordan, MHA
Retired Chief Executive Officer
Anne Arundel Medical Center

Margaret Hammersla, PhD
Senior Director DNP Program
Assistant Professor
Organizational Systems Adult Health
University of Maryland School of Nursing

Jason C. McCarthy, Pharm.D
Vice President of Operations – Baltimore
Kaiser Foundation Health Plan

Jeffrey Metz, MBA, LNHA
President and Administrator
Egle Nursing and Rehab Center

Gerard S. O'Connor, MD
General Surgeon in Private Practice

Michael J. O'Grady, PhD
Principal, Health Policy LLC, and
Senior Fellow, National Opinion Research Ctr (NORC) at the University of Chicago

Martha G. Rymer, CPA
Rymer & Associates, PA

Randolph S. Sergent, Esq.
Vice Chair, Maryland Health Care Commission
Vice President and Deputy General Counsel
CareFirst BlueCross BlueShield

Stephen B. Thomas, PhD
Professor of Health Services Administration
School of Public Health
Director, Maryland Center for Health Equity
University of Maryland, College Park

Marcus L. Wang, Esq.
Co-Founder, President and General Manager
ZytoGen Global Genetics Institute

Table of Contents

Introduction

The health care industry is among five industries at greatest risk of a data breach.[1] The most prominent contributors to the record-breaking number of breach occurrences and records compromised are external hacking attacks and internal threats.[2] Unlike other sectors of the economy, the majority of breaches in health care are tied to human error or abuse of access privilege.[3] Technology-related crime (i.e., cybercrime) and insider wrongdoing[4] lead to unauthorized and malicious use of patient information that can go undetected for from one day to several years.[5] The proliferation of cybercrime goes beyond data integrity and privacy; it increases risk to patient health and safety (e.g., ransomware that obstructs workflows and access to data).

Health care has generally been slower to embrace information technology (IT) and lags in data security[6] compared to other sectors such as banking and retail where IT has evolved organically over decades. Historically, health care mainly relied on electronic systems for billing and revenue cycle management. Since the expansion of federal government funding in 2009[7] efforts to digitize health care have accelerated dramatically as policymakers, clinical experts, and other stakeholders have sought to leverage technology to promote better care, improve outcomes, and reduce costs.[8] This movement ushered in a period of change. The most significant outcome from this movement was electronic health record (EHR)[9] technology becoming standard in care delivery.

Greater need for electronic exchange across health care organizations presents both benefits and risks.[10] New techniques that leverage technology (e.g., artificial intelligence, big data, machine learning, risk scoring, etc.) are advancing; at the same time, these techniques create new vulnerabilities. Evolving cyber threats, such as ransomware,[11] can interrupt operations and pose significant risks for health care organizations of all sizes. Ransomware halts workflows and data access, jeopardizing the ability for providers to make well-informed decisions about patient care. Continuous and comprehensive security monitoring, evaluation, and training are vital for health care organizations to reduce cyber risk and protect patient data.

About this Report

The Maryland Health Care Commission (MHCC) analyzed breaches affecting 500 or more individuals. Data was reported by covered entities (CE)[12] and business associates (BA)[13] from January 1, 2010 to October 18, 2019 and obtained from the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) online portal. Breaches are categorized as "archived" (i.e., breaches that have been investigated and closed, or with a reporting date older than 24 months) or "currently under investigation" (i.e., breaches with an open investigation).[14, 15] This review centers on Maryland in comparison to the nation as it relates to breach occurrences, estimated records compromised, breach type,[16] and entity type. Key findings highlight breach trends and are supported by available literature. This report is intended to provide stakeholders with a perspective about breaches in Maryland and the nation.

The information included in this report illustrates that health care breaches have become more commonplace. Reported breach occurrences continue to rise in Maryland and the nation. Data suggests that breach occurrences in Maryland are analogous to the average among all states. The evolving nature of cybercrime has heightened health care organizations' awareness of cybersecurity and spurred investments in hardware and software, employee training, continuous system monitoring, and incident response preparedness. The health care industry considers existing State and federal requirements for data privacy and security as generally adequate to safeguard protected health information (PHI)[17] and recognizes the need for health care organizations to bolster cybersecurity best practices. Breaches have shaped health care consumers' views about privacy and security. Health care organizations view preserving consumer trust and avoiding reputational harm as important justifications for implementing more robust cybersecurity protections.

Key Findings

A Snapshot of Open and Archived Breach Investigations

Table 1. Open Breaches						
Year	Nation			Maryland		
	Records	Occurrences	Percent Total (Records/ Occurrences)	Records	Occurrences	Percent Total (Records/ Occurrences)
2017	211,589	25	<1/4	0	0	0/0
2018	7,789,727	172	17/32	6,200	1	3/8
2019	39,170,430	351	83/64	182,416	11	97/92
Total	47,171,746	548	100/100	188,616	12	100/100

Notes: All data reflect open breaches from October 19, 2017 through October 18, 2019; see Tables 3 and 4 for total breach occurrences and records compromised.

A provision in the HITECH Act[18] requires CEs and BAs to notify the OCR of a breach (by filing an electronic report through the OCR online portal) within specified timeframes.[19] These reports offer insight into areas of vulnerability in protecting the privacy and security of PHI.[20] The OCR online portal includes information (historical and current) on reported breaches. Breaches currently under investigation,[21] as reported within the last 24 months, comprise more than 500 breaches in the nation and a dozen in Maryland.

Table 2. Archived Breaches						
Year	Nation			Maryland		
	Records	Occurrences	Percent Total (Records/ Occurrences)	Records	Occurrences	Percent Total (Records/ Occurrences)
2010	5,836,972	177	3/7	2,492	3	<1/6
2011	13,163,236	201	7/9	5,765	2	<1/4
2012	2,854,525	218	2/9	12,556	3	<1/6
2013	7,017,525	277	4/12	23,058	4	1/8
2014	17,503,206	315	9/13	273,719	6	10/13
2015	113,306,969	269	60/11	1,131,380	8	41/17
2016	16,659,090	329	9/14	669,919	6	24/12
2017	4,931,501	333	3/14	55,961	8	2/17
2018	6,155,014	199	3/8	582,854	8	21/17
2019*	477,357	33	<1/1	0	0	0/0
Total	187,905,395	2,351	100/100	2,757,704	48	100/100

*Notes: *Data through October 18, 2019; see Tables 3 and 4 for total breach occurrences and records compromised.*

Breach notification requirements aim to achieve two main objectives: increase public transparency and CE and BA accountability.[22] OCR enforcement may include compliance reviews, resolution agreements,[23] and corrective action.[24] HHS reports corrective action was obtained for a majority (83 percent)[25] of breach compliance reviews conducted in 2018.[26] In some cases, monetary enforcement is imposed if there is evidence of non-compliance, including inadequate privacy and security controls or untimely reporting to the OCR.[27] Overall, about 54 percent of breaches in 2018 and nine percent in 2019 have been investigated and closed (closed/total reported 2018: 199/371; 2019: 33/384). For Maryland, nearly 89 percent of breaches in 2018 have been closed; all breaches reported in 2019 remain open (closed/total reported 2018: 8/9; 2019: 0/11).

Reported Breaches at a Glance

Table 3. Total Breach Occurrences				
Year	Nation		Maryland	
	Occurrences	Percent Total	Occurrences	Percent Total
2010	177	6	3	5
2011	199	7	2	3
2012	218	8	3	5
2013	276	10	4	7
2014	313	11	6	10
2015	269	9	8	13
2016	329	11	6	10
2017	353	12	8	13
2018	369	13	9	15
2019*	384	13	11	19
Total	2,887	100%	60	100%

*Note: *Data through October 18, 2019.*[28]

The health care sector experienced an upward trend in breach occurrences over the past 10 years, averaging about one breach per day nationally (since 2017).[29] Since 2010, reported breaches in the nation and Maryland increased at a compound annual growth rate (CAGR) of 8.1 percent and 13.9 percent respectively. The number of breach occurrences reported (2010-2019) in Maryland represents about two percent of the national total and slightly exceeds the national average (55 breach occurrences).[30] The health care sector has made significant investments in cybersecurity over the last five years.[31] These investments are timely as cybercrime becomes increasingly sophisticated with new variants of malware capable of mining data[32] from health care systems and networks. Breach occurrences overall have increased at a slower rate since 2015.

Table 4. Total Records Compromised				
Year	Nation		Maryland	
	Records	Percent Total	Records	Percent Total
2010	5,836,972	2	2,492	<1
2011	13,160,857	6	5,765	<1
2012	2,854,525	1	12,556	<1
2013	7,016,139	3	23,058	1
2014	17,451,293	7	273,719	9
2015	113,306,969	48	1,131,380	38
2016	16,659,090	7	669,919	23
2017	5,123,671	2	55,961	2
2018	13,943,464	6	589,054	20
2019*	39,647,787	17	182,416	6
Total	235,000,767	100%	2,946,320	100%

*Note: *Data through October 18, 2019.*[33]

The amount of electronic health information has grown exponentially over the last decade creating new challenges in safeguarding PHI. In 2015, a more than six-fold increase in records compromised occurred nationally, representing a third of the U.S. population (records do not necessarily represent unique patients).[34] During that year, the majority of records compromised was attributed to a single breach.[35] Since then, there have been five high profile breach occurrences (three of which involved health plans) each ranging from 10 to 80 million records.[36] This includes the two largest breaches to date: one involving a health plan[37] and the other stemming from a BA that affected five CEs.[38] Maryland's largest breach[39] (2015) compromised just over one million records. The total number of records compromised in Maryland (2,946,320) represents about one percent of the nation and is below the average for all states (4,463,872 records).[40]

A Comprehensive Look at Breach Type

Table 5. Breach Type 2010-2019*								
Type	**Nation**				**Maryland**			
	Occurrence	*Percent Total (Occurrence)*	*Records*	*Percent Total (Records)*	*Occurrence*	*Percent Total (Occurrence)*	*Records*	*Percent Total (Records)*
Hacking/IT Incident	823	29	180,963,637	77	27	45	1,932,586	66
Improper Disposal	88	3	1,347,863	1	-	-	-	-
Loss	185	6	8,124,594	3	2	3	1,220	<1
Other	85	3	1,339,969	1	1	2	692	<1
Theft	871	30	25,270,294	11	10	17	78,976	3
Unauthorized Access/ Disclosure	824	29	16,036,951	7	20	33	932,846	32
Unknown	11	<1	1,917,459	1	-	-	-	-
Total	2,887	100%	235,000,767	100%	60	100%	2,946,320	100%

*Notes: *Data through October 18, 2019; a dash (-) signifies that no data was reported.*

Breaches resulting from hacking/IT incidents compromised a majority of records in the nation and Maryland. Cyber criminals are driven by diverse aims, including financial gain, challenge, revenge, subversion, and notoriety. Individuals that steal PHI are motivated to sell it on the black market. A full medical record[41] can sell for up to $1,000; in contrast, a social security number or credit card information usually sell for $100 or less.[42] This is because credit cards are much easier to replace than finding and establishing new trust relationships with health care providers. Nationally, theft accounts for the second largest percent of records compromised; unauthorized access/disclosure is the second breach type reported in Maryland responsible for about a third of records compromised, surpassing the nation by 25 percent. Records compromised from theft and unauthorized access/disclosure trail hacking/IT in contrast to breach occurrences overall in the nation. Hacking/IT is the most reported breach type in Maryland.

Table 6. Breach Type by Year Records Compromised								
Nation								
Year	*Hacking/IT Incident*	*Improper Disposal*	*Loss*	*Other*	*Theft*	*Unauthorized Access/Disclosure*	*Unknown*	*Total Records*
2010	92,358	34,587	921,109	156,933	4,010,716	620,501	768	5,836,972
2011	298,335	63,948	6,025,016	13,981	4,719,745	126,010	1,913,822	13,160,857
2012	907,751	21,830	98,064	514,833	958,668	353,379	-	2,854,525
2013	294,954	526,538	131,540	253,943	5,460,236	347,012	1,916	7,016,139
2014	6,370,313	106,562	211,297	400,279	7,229,344	3,132,545	953	17,451,293
2015	111,812,172	82,421	52,359	-	737,606	622,411	-	113,306,969
2016	13,428,313	125,730	557,952	-	904,451	1,642,644	-	16,659,090
2017	3,469,817	30,822	36,106	-	345,259	1,241,667	-	5,123,671
2018	9,394,218	342,272	29,966	-	693,006	3,484,002	-	13,943,464
2019*	34,895,406	13,153	61,185	-	211,263	4,466,780	-	39,647,787
Total	180,963,637	1,347,863	8,124,594	1,339,969	25,270,294	16,036,951	1,917,459	235,000,767
Maryland								
Year	*Hacking/IT Incident*	*Improper Disposal*	*Loss*	*Other*	*Theft*	*Unauthorized Access/Disclosure*	*Unknown*	*Total Records*
2010	1,000	-	-	692	800	-	-	2,492
2011	-	-	-	-	5,000	765	-	5,765
2012	-	-	-	-	11,924	632	-	12,556
2013	6,400	-	-	-	16,658	-	-	23,058
2014	10,766	-	620	-	42,713	219,620	-	273,719
2015	1,126,442	-	-	-	571	4,367	-	1,131,380
2016	17,041	-	-	-	-	652,878	-	669,919
2017	53,002	-	600	-	-	2,359	-	55,961
2018	555,441	-	-	-	1,310	32,303	-	589,054
2019*	162,494	-	-	-	-	19,922	-	182,416
Total	1,932,586	0	1,220	692	78,976	932,846	-	2,946,320

*Notes: *Data through October 18, 2019; a dash (-) signifies that no data was reported.*

A shift in breach type occurred in the nation following a 2014 surge in records compromised due to hacking/IT incidents. Subsequently in 2015, hacking/IT surpassed both theft and unauthorized access/disclosure for the first time in the nation and Maryland. Since then, hacking/IT has remained responsible for the bulk of all records compromised, accounting for more than 90 percent of records in the nation and 70 percent in Maryland (2015-2019). Improving security posture is a priority in health care.[43] Identifying and addressing network vulnerabilities is essential to stemming the growth of hacking/IT incidents. Unauthorized access/disclosure continues to be a prevailing breach type, particularly in Maryland where it accounts for over a quarter of records compromised between 2015 and 2019, compared to six percent in the nation.

Table 7. Breaches by CE Type
2010-2019*

Type	Nation		Maryland	
	Records	*Percent Total (Records)*	*Records*	*Percent Total (Records)*
Business Associate	51,823,706	22	72,209	2
Health Plan	116,619,755	50	1,429,959	49
Health Care Provider	64,951,833	28	1,444,152	49
Healthcare Clearinghouse	1,584,692	<1	-	-
Unknown	20,781	<1	-	-
Total	235,000,767	100%	2,946,320	100%

*Notes: *Data through October 18, 2019; dash (-) signifies that no data was reported.*

HITECH extends HIPAA breach notification provisions to BAs.[44] BAs are entities that perform functions using PHI on behalf of a CE and can include health IT vendors, billing companies, and collection services. In 2019, three of the five largest breaches among BAs nationally resulted from a phishing[45] email.[46] Layered IT systems and a multitude of connected devices make health care providers appealing to cyber criminals.[47] It's estimated that hospitals experience up to 70 percent of all ransomware attacks.[48] The growing prevalence of these attacks where data is held hostage until a ransom is paid or systems have been restored from backups can have a devastating effect on operations, even impacting patient health and safety. Health plans are responsible for almost half of the total records compromised in the nation[49] and Maryland[50], largely due to the volume of PHI contained across their networks.

Table 8. Breaches by CE Type by Year						
Nation						
Year	*BA*		*Health Plan*		*Health Care Provider*	
	Occurrences	Records	Occurrences	Records	Occurrences	Records
2010	36	1,498,167	20	3,560,444	121	778,361
2011	44	8,935,715	20	90,537	134	4,133,355
2012	40	1,146,711	23	336,265	154	1,361,549
2013	64	1,058,760	18	97,555	191	5,853,320
2014	77	12,988,487	41	2,247,146	193	2,197,061
2015	14	3,992,767	61	102,919,905	194	6,394,297
2016	22	3,564,666	51	880,455	256	12,213,969
2017	21	212,754	51	347,558	281	4,563,359
2018	42	5,980,018	53	2,833,971	273	5,127,293
2019*	43	12,445,661	46	3,305,919	293	22,329,269
Total	403	51,823,706	384	116,619,755	2,090	64,951,833
Maryland						
Year	*BA*		*Health Plan*		*Health Care Provider*	
	Occurrences	Records	Occurrences	Records	Occurrences	Records
2010	1	800	1	692	1	1,000
2011	1	765	-	-	1	5,000
2012	2	2,076	-	-	1	10,480
2013	-	-	-	-	4	23,058
2014	1	10,766	3	219,620	2	43,333
2015	-	-	3	1,102,105	5	29,275
2016	-	-	-	-	6	669,919
2017	1	664	-	-	7	55,297
2018	-	-	2	20,142	7	568,912
2019*	3	57,138	1	87,400	7	37,878
Total	9	72,209	10	1,429,959	41	1,444,152

*Notes: *Data through October 18, 2019; dash (-) signifies that no data was reported; breaches reported by clearinghouses or with unknown information are not included.*

Over the last decade, breach occurrences reported by health plans and health care providers have more than doubled in the nation as compared to BAs. Health care providers may be more susceptible to a breach in part due to limited resources to measure cybersecurity readiness and to conduct mock exercises, among other things.[51, 52] A large volume of records compromised by health plans in Maryland can be attributed a single breach.[53] In 2015, Anthem reported the largest breach to date that resulted from a phishing email and enabled unauthorized access to at least 90 systems across the enterprise.[54] An investigation found that prior to the breach, Anthem had taken reasonable measures to protect data, which included a remediation plan that resulted in a rapid response after discovery of the breach.[55] Greater need to bolster cybersecurity is propelling CEs to adopt security frameworks[56] that go beyond minimum requirements for privacy and security established by HIPAA.[57] These frameworks identify best practices that reduce intrusion risks to IT systems.

An Overview of Breaches by State

Table 9. State Totals 2010-2019*					
State	**Records**	**Occurrences**	**State**	**Records**	**Occurrences**
AK	75,785	11	MT	1,194,989	16
AL	1,576,471	37	NC	13,537,108	70
AR	604,133	34	ND	17,515	6
AZ	4,881,285	66	NE	295,569	24
CA	10,454,846	302	NH	266,183	8
CO	339,954	57	NJ	3,849,967	52
CT	1,189,111	47	NM	275,268	26
DC	52,495	11	NV	293,209	26
DE	108,737	7	NY	18,389,999	157
FL	7,589,611	179	OH	1,194,992	97
GA	3,841,559	87	OK	635,539	26
HI	55,136	5	OR	460,763	52
IA	1,607,414	31	PA	2,235,292	102
ID	26,462	5	PR	1,710,315	30
IL	4,959,796	135	RI	111,810	18
IN	84,961,857	87	SC	866,985	29
KS	307,045	24	SD	36,900	8
KY	1,088,404	60	TN	11,873,570	70
LA	281,116	26	TX	8,273,162	239
MA	670,842	81	UT	1,377,994	19
MD	2,946,320	60	VA	8,837,342	46
ME	45,362	8	VT	79,788	7
MI	1,079,962	78	WA	13,307,763	75
MN	12,161,212	82	WI	670,017	42
MO	1,066,233	69	WV	89,809	14
MS	205,711	19	WY	62,621	10

*Notes: *Data through October 18, 2019; data includes all 50 states, the District of Columbia and Puerto Rico.*

Reported breaches are disproportionately distributed across states largely because breaches at health plans, the CE affected most by large breaches, cover individuals residing in multiple states; however, the OCR attributes these breaches to the state reporting the breach. Records compromised are based on organization size and magnitude of a breach.[58] The top 10 states with the highest number of breach occurrences and records compromised from 2010 through 2019 have larger populations (excludes Maryland).[59, 60] Six states[61] are among the top 10 for both breach occurrences and records compromised. Variation exists in the top 10 states by individual year (2010 through 2019), which includes Maryland once for breach occurrences and four times for records compromised;[62] Maryland appeared in the top 10 for both occurrences and records in 2015. Most states have laws on data breach notification to consumers and their Attorney General's Office;[63] about 40 percent of states have laws where medical information is subject to breach notification processes.[64] These laws are more stringent than HIPAA on the timing of breach notification and requirements for providing credit monitoring and identity theft protection services to breach victims.[65] Amendments to Maryland's Personal Information Protection Act (PIPA),[66] effective January 2018, expand breach notification to include information covered under HIPAA, such as health information, health insurance policy information, and biometric data. PIPA holds organizations operating in the State liable for ensuring privacy and security.[67]

Privacy and Security - Consumers Perspective

Many consumers (70 percent) believe their personal information is less secure today than it was five years ago.[68] Breaches erode public trust and motivate health care organizations to reduce information security risks.[69] One in four (26 percent) consumers have been victim of a health care data breach, half of which experienced medical identity theft as a result.[70] The estimated percent of consumers victimized by a breach is likely much higher given the millions of records compromised to date.[71] Consumers whose medical information is compromised are less likely to stop dealing with the organization responsible for the breach in comparison to those whose credit card information was compromised (27 percent and 37 percent, respectively).[72]

Large scale and high profile data breaches are shifting public sentiment on privacy and security. Consumer attitudes vary by the type of personal information (e.g., financial/banking, health, biometrics, etc.) they view as private.[73] Health information ranks fourth (61 percent) among personal information that consumers feel should have greater protections.[74] Consumers rely on health care organizations to be good stewards of their PHI.[75] Privacy and security are viewed by consumers as most important when visiting a health care provider.[76] Health care providers (in addition to banks) are trusted more by consumers when it comes to privacy and security as compared to advertising, online retailers, social media, etc.[77, 78]

Implementing transparent and robust defenses to protect personal information can alleviate consumer concerns and the potential impact on their privacy.[79] Consumers fear cyber-attacks that result in a health data breach (59 percent) more so than risk of unauthorized access to medical devices[80] (41 percent).[81] Patient portals have increased consumer concerns about the ease in which PHI can be accessed.[82] One in four patient portal users worry about unauthorized access to their personal information.[83] Certain breach response measures satisfy consumers' more than financial compensation; these include safeguarding against future breaches, free credit monitoring, and timely notification to consumers.[84]

Consumers' desire to protect their personal information is understandable as demographic, financial, and clinical data can be exploited for nefarious purposes.[85, 86] Increasingly, consumers are more aware of the likelihood of being victim to a breach; more than half of consumers (64 percent) are inclined to blame companies for exposing their personal information.[87] Lessons learned in the aftermath of a breach are the underpinnings to improve security dialogue enterprise-wide, strengthening security posture, and consumer trust. Health care organizations' response to a breach is just as important as what they may or may not have done to prevent it.

Vigilance – Key to Avoiding Breaches

A prevailing theme for safeguarding PHI is to remain vigilant. Breaches can have a devastating impact on business continuity, patient safety, and cost.[88, 89] Greater need for electronic data exchange presents opportunities for cyber criminals to exploit vulnerabilities, an intractable part of the cybersecurity landscape. Nearly all vulnerabilities (99 percent) are publicly known before a cyber-attack takes place.[90] Ensuring privacy and security of patient data requires an understanding and resolution of past challenges to prepare for new and evolving cyber threats. Best practices include ongoing auditing of systems and processes to identify potential weaknesses, ensuring BAs maintain stringent security measures, backing up systems and testing backup restoration routinely, and increasing awareness of cybersecurity among all employees.[91] Future innovation requires greater collaboration and use of connected technology. Protecting data necessitates adaptable security protocols to address impending cybersecurity threats on the horizon.

Limitations

Breach data is self-reported by CEs and BAs to the OCR and may be updated if additional information is discovered that supplements, modifies, or clarifies a previous submission. Breach data obtained from the OCR does not specify report type (i.e., initial breach report or addendum to previous report). CEs and BAs report an estimate of records compromised, which may be the total number of records in a system. CEs may report a breach on behalf of a BA and more than one breach type may be reported for a single breach.[92] Errors and omissions in data reporting are unknown as data validation was not possible in this analysis. The number of archived breaches that are under investigation is not made available by the OCR. Information on breaches impacting fewer than 500 individuals is not publicly available.

Appendix

State Rankings *Top 10* 2010-2019*					
Rank	**State** (State Population Ranking)	**Records**	*Rank*	**State** (State Population Ranking)	**Occurrences**
1	IN (17)	84,961,857	1	CA (1)	302
2	NY (4)	18,389,999	2	TX (2)	239
3	NC (9)	13,537,108	3	FL (3)	179
4	WA (13)	13,307,763	4	NY (4)	157
5	MN (22)	12,161,212	5	IL (6)	135
6	TN (16)	11,873,570	6	PA (5)	102
7	CA (1)	10,454,846	7	OH (7)	97
8	VA (12)	8,837,342	8	IN (17)	87
9	TX (2)	8,273,162	9	GA (8)	87
10	FL (3)	7,589,611	10	MN (21)	82

*Note: *Data through October 18, 2019.*

[1] Remaining top 5 industries include the public sector, accommodation, retail and finance. More information available at: enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.
[2] The large daily volume of accesses to health data poses challenges in determining anomalies indicative of account misuse or a cyberattack. More information available at: www.hipaajournal.com/vulnerabilities-in-servers-behind-majority-of-healthcare-data-breaches/.
[3] Verizon, *2019 Data Breach Investigations Report,* May 2019. Available at: enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.
[4] Insider wrongdoing is generally categorized under unauthorized access/disclosure.
[5] Protenus, *Protenus 2019 Breach Barometer*, 2019. Available at: email.protenus.com/hubfs/Breach_Barometer/2018/2019%20Breach%20Barometer%20Annual%20Report.pdf.
[6] Kruse C, Frederick B, Jacobson T, Monticone D. Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends, *Technology and Health Care* 2017; 25(1): 1-10.
[7] The Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 broadly subsidized electronic health record adoption among providers. More information available at: www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html.
[8] Gold M, McLaughlin C. Assessing HITECH Implementation and Lessons: 5 Years Later. *Milbank Q*. 2016; 94(3): 654–687.
[9] An EHR is a real-time patient health record with medical and treatment histories of patients and access to evidence-based decision support tools; it can also support the collection of data for uses other than clinical care such as billing, quality management, outcome reporting, etc.
[10] Health Care Industry Cybersecurity Task Force, *Report on Improving Cybersecurity in the Health Industry,* June 2017. Available at: www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.
[11] Ransomware is a type of malware designed to deny access to a computer system or data until a ransom is paid.
[12] CEs include health plans, health care clearinghouses, health care providers, and business associates. More information available at: www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html.
[13] BAs include entities that create, receive, maintain, or transmit PHI on behalf of a CE or another BA.
[14] After 24 months from the date a breach is reported, OCR archives the breach. Archived breaches may still have an open investigation.
[15] Breaches under investigation/archived as of October 18, 2019: Nation 548/2,351; Maryland 12/48.
[16] Breach type includes hacking/IT incident, improper disposal, loss, theft, unauthorized access/disclosure, unknown, and other.
[17] PHI may include information that is demographic (e.g., name, e-mail, date of birth, social security number, etc.), financial (e.g., service dates, payment method, etc.), or clinical (e.g., diagnoses, prescriptions, treatment, etc.).
[18] HITECH promoted and expanded adoption of health IT, specifically EHRs, and introduced penalties for CEs and BAs that are not compliant with the Health Insurance Portability and Accountability Act (HIPAA). More information available at: www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html.
[19] CEs and BAs must notify OCR within 60 days from discovery of a breach affecting more than 500 individuals; breaches affecting fewer than 500 individuals must be reported within 60 days of the end of the calendar year. More information available at: www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html.
[20] U.S. Department of Health & Human Services, *Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance For Calendar Years 2015, 2016, and 2017*. Available at: www.hhs.gov/sites/default/files/compliance-report-to-congress-2015-2016-2017.pdf.
[21] Breaches that have been closed or are older than 24 months are archived.
[22] U.S. Department of Health & Human Services, *Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Years 2015, 2016, and 2017*. Available at: www.hhs.gov/sites/default/files/breach-report-to-congress-2015-2016-2017.pdf.
[23] A resolution agreement is a settlement agreement signed by HHS and a CE or BA in which the CE or BA agrees to perform certain obligations and make reports to HHS, generally for a period of three years. A resolution agreement may include the payment of a resolution amount. More information available at: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.
[24] OCR investigates and provides technical assistance to or requires a CE or BA to make changes regarding HIPAA-related privacy and security policies, procedures, training, or safeguards. More information available at: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/index.html.
[25] Outcome for 359 out of 431 resolutions resulting from breach compliance reviews.
[26] U.S. Department of Health & Human Services, *Enforcement Results by Year,* April 2019. Available at: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html#ir2018.
[27] See n. 24, *Supra.*
[28] Total is 12 less occurrences that were duplicative in Tables 1 and 2, Open and Archived Breaches.
[29] As of 2018, average time to breach discovery was about 255 days. More information available at: email.protenus.com/hubfs/Breach_Barometer/2018/2019%20Breach%20Barometer%20Annual%20Report.pdf.
[30] National average includes District of Columbia and Puerto Rico. See Table 9 for number of breach occurrences by all states.
[31] See n. 10, *Supra.*
[32] Data mining refers to the process of identifying patterns in large datasets.
[33] Total is one percent fewer records compromised that were duplicative in Tables 1 and 2, Open and Archived Breaches.
[34] CSO, *Over 113 million health records breached in 2015 – up 10-fold from 2014,* January 2016. Available at: www.csoonline.com/article/3026661/over-113-million-health-records-breached-in-2015-up-10-fold-from-2014.html.
[35] Nation: Anthem (70 percent); Maryland: CareFirst BlueCross BlueShield (97 percent).
[36] 2015: Anthem (78.8 million records), Premera Blue Cross (11 million records), Excellus Blue Cross Blue Shield (10 million records); 2019: Optum 360 (11.5 million records); LabCorp (10 million records).
[37] The breach occurred in 2015 at Anthem and impacted 50 accounts and 90 systems across the enterprise. Approximately 78.8 million records were compromised. More information available at: www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627.
[38] The breach occurred in 2019 at American Medical Collection Agency (BA). Five CEs reported the breach to OCR including: Quest Diagnostics, MN (11.5 million records), LabCorp, NC (7.7 million records), CompuNet Clinical Laboratories, OH (111,000 records), Inform Diagnostics, TX (173,690 records), and West Hills Hospital & Medical Center (number of records not yet disclosed). More information available at: www.advisory.com/daily-briefing/2019/08/13/data-breach.
[39] The breach occurred at CareFirst BlueCross BlueShield and compromised 1.1 million records.
[40] National average includes District of Columbia and Puerto Rico. See Table 9 for records compromised by all states.
[41] Individuals who purchase medical information on the black market may use it to purchase medical equipment or drugs, or file false insurance claims. More information available at: www.medidfraud.org/.

[42] Advisory Board, *What hackers actually do with your stolen medical records*, March 2019. Available at: www.advisory.com/daily-briefing/2019/03/01/hackers.
[43] The Healthcare Information and Management Systems Society (HIMSS) conducted a survey of health information and technology professionals in 2019 on leadership priorities found that *Cybersecurity, Privacy, and Security* were rated as top priorities by vendors and providers. More information available at: www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_US_LEADERSHIP_WORKFORCE_SURVEY_Final_Report.pdf.
[44] OCR issued a final rule in 2013 to modify the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules. Among other things, the final rule identifies provisions of the HIPAA Rules that apply directly to BAs and for which BAs are directly liable. More information available at: www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html#footnote2_dj90coq.
[45] Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity or contact, generally via email.
[46] Calyptix Security, *5 Biggest Data Breaches at HIPAA Business Associates in 2019 (So Far)*, May 2019. Available at: www.calyptix.com/hipaa/5-biggest-data-breaches-at-hipaa-business-associates-in-2019-so-far/.
[47] See n.10, *Supra.*
[48] Inside Sources, *Hospitals Are Cyber Criminals' Newest, Biggest Target*, February 2019. Available at: www.insidesources.com/hospitals-are-cyber-criminals-newest-biggest-target/.
[49] Three of the five largest breaches reported were hacking/IT incidents targeting health plans that compromised nearly 100 million records.
[50] Records compromised due to breaches reported by health care providers surpass health plans by 14,193 records in Maryland (2010 – 2019).
[51] Cision, *Healthcare Data Breaches Costs Industry $4 Billion by Year's End, 2020 Will Be Worse Reports New Black Book Survey,* November 2019. Available at: www.prnewswire.com/news-releases/healthcare-data-breaches-costs-industry-4-billion-by-years-end-2020-will-be-worse-reports-new-black-book-survey-300950388.html.
[52] In 2019 Black Book Market Research LLC surveyed nearly 2,900 security professionals from provider organizations and found that nearly half (40 percent) of providers do not carry out measurable assessments of their cybersecurity status, and the majority (87 percent) of health care organizations do not conduct cybersecurity drills with an incident response process. More information available at: blackbookmarketresearch.newswire.com/news/healthcare-data-breaches-costs-industry-4-billion-by-years-end-2020-21027640.
[53] Health plans: Nation – Anthem (68 percent); Maryland – CareFirst BlueCross BlueShield (77 percent).
[54] Anthem has reportedly incurred significant costs related to the breach, including $2.5 million to engage expert consultants; $115 million to implement security improvements; $31 million to provide notification to the public and affected individuals; and $112 million to provide credit protection to impacted consumers. More information available at: www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627.
[55] Bank Info Security, *A New In-Depth Analysis of Anthem Breach,* January 2017. Available at: www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627.
[56] A security framework is a proven approach to developing policies and procedures to enhance security strategies (assessing current and desired state, identifying gaps in risk management programs, providing specific tools and resources, etc.) for securing systems and data.
[57] For example, Anthem was certified in 2013 as compliant with the HITRUST (Health Information Trust Alliance) Common Security Framework. More information available at: www.bankinfosecurity.com/analysis-did-anthems-security-certification-have-value-a-11634.
[58] About half of states (27) did not report any breaches in at least one or more years since 2010.
[59] See Appendix for state rankings (2010-2019).
[60] Data exposed from a breach can include residents from other states.
[61] CA*, FL*, IN, MN, NY*, TX*. An asterisk (*) notes those states that are the most populated (top four) in the U.S.
[62] Maryland breach occurrences ranking: 8th (2015). Maryland records compromised ranking: 7th (2014); 5th (2015); 6th (2016); 10th (2018).
[63] The Attorney General's Office in several states has the authority to enforce the law, including but not limited to civil penalties and other actions to address reported violations and for other relief that may be appropriate. More information available at: www.foley.com/en/insights/publications/2019/01/-/media/409938b300d2452a85671df61679acf8.ashx.
[64] Foley & Lardner LLP, *State Data Breach Notification Laws,* October 2019. Available at: www.foley.com/en/insights/publications/2019/01/-/media/409938b300d2452a85671df61679acf8.ashx.
[65] *Ibid.*
[66] PIPA (Md. Code Ann. Comm. Law 14-3504) requires notification to be sent to all Maryland residents affected by a breach. Notification must be issued as soon as practicable but no later than 45 days after discovery of a breach. More information available at: www.marylandattorneygeneral.gov/Pages/IdentityTheft/businessGL.aspx.
[67] HIPAA Journal, *Maryland Data Breach Notification Law Updated*, August 2017. Available at: www.hipaajournal.com/maryland-data-breach-notification-law-updated-8915/.
[68] Individuals over age 50 are more likely to think their data is less secure compared with those ages 18 to 49. More information available at: www.pewresearch.org/internet/2019/11/15/how-americans-think-about-privacy-and-the-vulnerability-of-their-personal-data/.
[69] Rand Corporation, *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*, 2016. Available at: www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf.
[70] Half of these victims were made aware of a breach after finding an error on their credit card statement or explanation of benefits. More information available at: newsroom.accenture.com/subjects/technology/one-in-four-us-consumers-have-had-their-healthcare-data-breached-accenture-survey-reveals.htm.
[71] RSA, *RSA Data Privacy & Security Survey 2019*, 2019. Available at: www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf.
[72] More information available at: www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf.
[73] See n. 71, *Supra.*
[74] Types of information consumers care about ahead of medical information include financial/banking data, security information, and identity information. More information available at: www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf.
[75] Consumers view their medical record as most important to keep out of the public eye as compared to email, social media, etc. More information available at: www.healthpopuli.com/2017/05/24/consumer-trust-deficit-health-engagement/.
[76] Visiting a health care provider is followed by using social media, performing Internet searches, and filing tax returns. More information available at: www.healthpopuli.com/2017/05/24/consumer-trust-deficit-health-engagement/.
[77] Hospitals and banks tie as most trusted. More information available at: www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf.
[78] Harvard T.H. Chan School of Public Health, *Americans' Views on Data Privacy & E-Cigarettes*, August 2019. Available at: cdn1.sph.harvard.edu/wp-content/uploads/sites/94/2019/08/Politico-HSPH-Data-Privacy-E-Cig-Report-081519.pdf.
[79] Martin K, Borah A, Palmatier R. Data Privacy: Effects on Customer and Firm Performance, *Journal of Marketing* 2017; 81(1): 36-58.

[80] Medical devices collect data and automate exchange providing insights into patient symptoms and enabling remote care.
[81] Morphisec, *Morphisec 2019 Consumer Healthcare Cybersecurity Threat Index*, 2019. Available at: www.morphisec.com/hubfs/1111/whitepapers/Morphisec-2019-Healthcare-Cyberthreats-Index-190401.pdf?utm_campaign=Healthcare%20Survey%20Report&utm_source=hs_automation&utm_medium=email&utm_content=71379354&_hsenc=p2ANqtz--LTW2MN53emryoN83ya9S5Jy-S0O1oTsZDGB7BM0jNmZ0hlUTVHrKmJqvEjNitarwh25kaASF9ywL_dV3cWvBChQgNAw&_hsmi=71379354.
[82] Consumers' use of patient portals are elevating their concerns about activity within their medical information. Consumers typically contact providers for an explanation; if they don't receive a response, they're likely to request assistance from OCR.
[83] See n. 78, *Supra.*
[84] Measures viewed least-satisfactory by consumers are donating money to organizations that promote cybersecurity and simply apologizing to those affected. More information available at: www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf.
[85] The more data a business collects about consumers, particularly sensitive data like PHI, the more lucrative that data becomes for cyber criminals. Recurring data exposures have enabled cyber criminals to more easily construct digital identities.
[86] See n. 10, *Supra.*
[87] See n. 71, *Supra.*
[88] American Hospital Association, *The importance of cybersecurity in protecting patient safety*. Available at: www.aha.org/center/emerging-issues/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety.
[89] Health care organizations bear more costs resulting from a data breach (about 60 percent higher than the cross-industry average). This includes cost of breach detection, business downtime, notification to affected individuals, post-breach response and recovery activities, reputational damage, and the impact on consumer trust. More information available at: databreachcalculator.mybluemix.net/.
[90] Calyptix Security, *Cyber Mistakes in Healthcare: Vulnerabilities and Misconfigs,* August 2018. Available at: www.calyptix.com/hipaa/cyber-mistakes-in-healthcare-vulnerabilities-and-misconfigs/.
[91] Managed Healthcare Executive, *Four Best Practices to Help Prevent Healthcare Cyberattacks*, January 2018. Available at: www.managedhealthcareexecutive.com/mhe-articles/four-best-practices-help-prevent-healthcare-cyberattacks. .
[92] Reporting entities were only counted once in this analysis.

David Sharp, PhD

Director

Center for Health Information Technology and Innovative Care Delivery

4160 Patterson Avenue

Baltimore, MD 21215

410-764-3460

www.mhcc.maryland.gov