Health Care Data Breaches:

How Maryland Compares

December 2017

Robert E. Moffit, PhD, Chair

Ben Steffen, Executive Director

Maryland Health Care Commission

MARYLAND
HEALTH CARE
COMMISSION

Table of Contents

Introduction

Health care data breaches are at an all-time high nationwide, with the majority resulting from hacking/information technology (IT) related incidents.[1] Such occurrences peaked in 2014 and were followed by several breaches in 2015 that compromised the greatest number of records to date in Maryland and the nation.[2] Growing security threats can be attributed to greater diffusion of electronic health information as health care becomes increasingly dependent on various electronic systems to manage patient medical records and perform billing and other administrative functions. Implementing safeguards to protect software and operating systems is essential; equally important is changing behavior by end-users of these systems to reduce the risk of a breach. Weaknesses in cybersecurity awareness and training exacerbate evolving threats, such as ransomware, which holds systems hostage, impeding or preventing patient care, though not always resulting in a breach.

Privacy and Security Rules

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[3] as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, contains standards for the protection of protected health information (PHI).[4] HIPAA established a floor for privacy and security protections of PHI. HITECH later expanded the scope of these protections and enhanced enforcement measures for covered entities (CE)[5] and business associates (BA)[6] that must comply with HIPAA. The HIPAA Omnibus Final Rule, adopted in 2013, strengthens privacy and security requirements and holds BAs and their subcontractors to the same standards as CEs. It also increases monetary penalties[7] for non-compliance and requires notification of breaches to the Department of Health & Human Services Office for Civil Rights (OCR).[8]

About this Report

The Maryland Health Care Commission (MHCC) conducted an all-state analysis[9] of health care breaches from 2013 through 2016[10] and a prospective review of breaches in 2017.[11] Data was obtained from the OCR online portal.[12] This report presents Maryland's ranking in relation to other states and serves as a supplement to MHCC's June 2017 report, *Health Care Data Breaches: A Changing Landscape,*[13] which

[1] Hacking incidents include phishing emails that seek sensitive information or attempts to gain unauthorized remote access to a network from a sophisticated adversary determined to find a point of entry.

[2] Nation: Anthem BlueCross (78M records); Premera BlueCross (11M records); Excellus BlueCross BlueShield (10M records). Maryland: CareFirst BlueCross BlueShield (1.1M records).

[3] Pub. L. 104-191, Aug. 21, 1996, 110 Stat. 1936.

[4] PHI includes information such as health status, provision of health care, or payment for health care that is transmitted or maintained in any form or medium created or collected by a covered entity or its business associate.

[5] CEs include health plans, health care clearinghouses, and health care providers. For more information: hhs.gov/hipaa/for-professionals/breach-notification/index.html.

[6] An entity qualifies as a BA if it creates, receives, maintains or transmits PHI on behalf of a CE or another business associate through the use of a technology or methodology specified by the Secretary in guidance.

[7] Fines for non-compliance are based on the level of negligence and range from $100 to $50,000 per violation (or record).

[8] 45 C.F.R. Parts 160, 164. Available as originally published at: gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf, or at www.ecfr.gov.

[9] Also includes the District of Columbia and one U.S. territory, Puerto Rico.

[10] Maryland: N=23; Nation: N=1,177

[11] Data for 2017 is from January 1st through November 6th and includes reported breaches closed (Maryland: N= 2; Nation: N= 34) and under investigation (Maryland: N=6; Nation: N=256).

[12] The portal includes details such as name of CE, state, CE type, number of individuals affected, breach submission date, type of breach, and location of breached information. For more information: ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[13] Maryland Health Care Commission, *Health Care Data Breaches: A Changing Landscape,* June 2017. Available at: mhcc.maryland.gov/mhcc/pages/hit/hit/documents/HIT_DataBreachesBrief_Brf_Rpt_090717.pdf.

assessed Maryland breaches by CE and breach type in comparison to the national average. This report provides a more detailed evaluation of records compromised and location of breached information to support MHCC in planning for health system needs and promoting informed decision making, among other things. Findings in this report will be used by MHCC in developing cybersecurity education and awareness initiatives.

Limitations

Findings are based on self-reported data from CEs and BAs for breaches affecting 500 or more individuals that have been investigated and closed by OCR.[14] The analysis does not include a comprehensive view of the origins and impact of all breaches as information on smaller breaches affecting fewer than 500 individuals is not available on the OCR online portal. Actual occurrence of breaches by year may vary as breaches are tracked by OCR based on the date a CE or BA reports a breach. Although OCR requires a breach to be reported within 60 days of discovery, timing of breach discovery may take much longer after a security incident has occurred.[15] OCR breach data does not include breach specifics related to origin or cause (e.g. ransomware, phishing, etc.). Trends identified in 2017 are based, in part, on preliminary data for breaches still under investigation; findings are subject to change once OCR completes its investigation of these breaches.

Trends

In recent years, the health care industry has become a prime target for cyberattacks with growth in breaches caused by hacking/IT far surpassing other breach types (Figure 1).[16, 17, 18] From 2013 to 2016, Maryland and the nation experienced a noticeable surge in hacking/IT breaches. Occurrences more than doubled, accounting for half of all breaches as of 2016 (Table 1). Such incidents have become more widespread due to the rise in ransomware[19] that often is initiated through a phishing scam. This is noteworthy because much attention is often given to vulnerabilities in software and operating systems, which, if exploited, can give a hacker access to PHI. Phishing scams do not exploit vulnerabilities in a system, rather they attempt to exploit vulnerabilities of individuals using the system. It is estimated that 91 percent of cyberattacks begin with a successful phish.[20]

[14] OCR updated its online portal in July 2017, making available breaches currently under investigation in addition to other features. For more information: hipaajournal.com/ocr-data-breach-portal-update-highlights-breaches-investigation-8897/.

[15] The Breach Barometer Report for 2016 by Protenus found that a health care organization discovers a data breach an average of 233 days to after the breach. For more information, visit: protenus.com/hubfs/Breach_Barometer/Protenus%20Breach%20Barometer-2016%20Year%20in%20Review-%20final%20version.pdf.

[16] See Appendix A for OCR definitions of breach type and breach location.

[17] Compound Annual Growth Rate 2014-2016 (%): Hacking/IT incidents (92); Theft (-24); Unauthorized Access/Disclosure (32).

[18] See n. 13, *Supra*.

[19] Ransomware is a type of malware (malicious software) that attempts to deny access to data usually by encrypting the data with a key only known by the hacker. A ransom is demanded to be paid in order to receive the decryption key. Ransomware attacks commonly start off with a phishing email, a fraudulent message that can gain system access by manipulating individuals into divulging confidential information.

[20] HIPAA Journal, *Hacking and Phishing Attacks Continue to Plague Healthcare Organizations*, February 2017. Available at: www.hipaajournal.com/hacking-phishing-attacks-continue-plague-healthcare-organizations/.

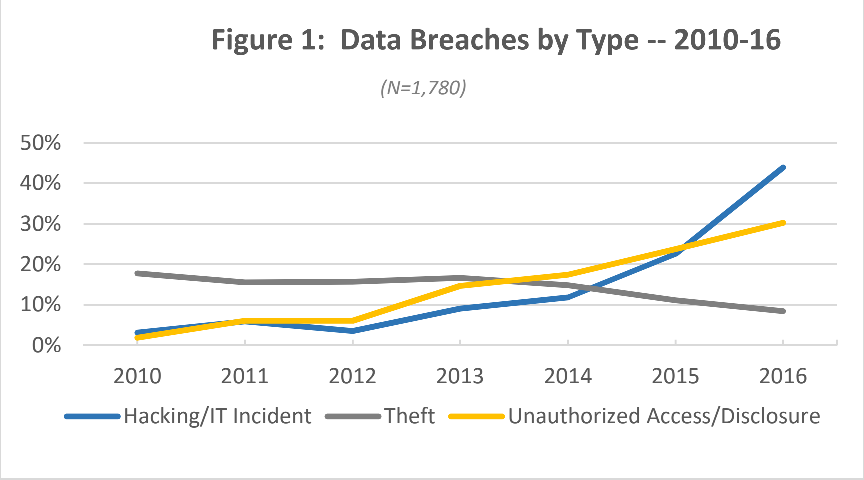

Figure 1: Data Breaches by Type -- 2010-16

(N=1,780)

Table 1: Breach Occurrences for Hacking/IT

Year	Maryland *n=8*		Nation *n=221*	
	#	%	#	%
2013	0	0	23	10
2014	1	13	30	14
2015	3	38	57	26
2016	4	50	111	50

Note: Overall, hacking/IT accounted for about 35 percent of all breaches in Maryland and 19 percent of all breaches nationally from 2013 to 2016.

Occurrences of unauthorized access/disclosures continue to increase and account for more breaches in Maryland and the nation; however, growth rate for this breach type has been more moderate as compared to hacking/IT.[21] While breaches involving theft have historically been highest, reports of this breach type have been on the decline since 2013.[22] More breaches resulting from hacking/IT and unauthorized access/disclosures can be attributed to the increased threat of adversaries (both internally[23] and externally) exploiting weaknesses in a digital health care infrastructure that is dependent on electronic systems, including cloud-based technology.

Health care providers in all states are most vulnerable, increasingly reporting well over 50 percent of all breaches.[24] In 2016, Maryland was one of fifteen states[25] (roughly 30 percent of all states) where providers accounted for all reported breaches.[26] Increased risk of a breach for providers can, in part, be attributed to varying levels of experience in using electronic information systems and implementing privacy and security

[21] Compound Annual Growth Rate 2014-2016 (%): Hacking/IT incidents (92); Theft (-24); Unauthorized Access/Disclosure (32).

[22] Breaches involving theft (#) – Nation: 2013 (121), 2014 (108), 2015 (81), 2016 (61); Maryland: 2013 (3); 2014 (1); 2015 (1); 2016 (0).

[23] The Breach Barometer 2016 report by Protenus found that 43 percent of breaches were due to insider error and insider malicious intent. For more information, visit: protenus.com/hubfs/Breach_Barometer/Protenus%20Breach%20Barometer-2016%20Year%20in%20Review-%20final%20version.pdf.

[24] The OCR online portal includes an option labeled, "Are you a CE filing on behalf of a BA?" Some CEs may not select that option because they incorrectly believe they are not filing on a BA's behalf.

[25] Includes Alaska, Arizona, District of Columbia, Iowa, Kansas, Massachusetts, Missouri, North Carolina, New Hampshire, Nevada, Rhode Island, Utah, Virginia, and Wyoming.

[26] Ambulatory practices, hospitals, and outpatient facilities are the most common provider types required by OCR to implement corrective actions to achieve HIPAA compliance.

controls.[27] The depth of this problem is even more diffuse because of the industry's growing emphasis on interconnectability among new and legacy electronic systems and networks while striving to meet the demands of evolving care redesign initiatives that place greater demands on those very systems and networks.

Maryland breaches tend to affect a smaller number of individuals, with a median[28] of 1,444 records per breach, as compared to an average median of 2,300 across all states. However, total records compromised in Maryland exceeds totals in most states for most breach types. Maryland ranks 9th for hacking/IT, 14th for theft, and 2nd for unauthorized access/disclosures.[29] In August 2016, OCR announced plans to broadly investigate smaller breaches affecting fewer than 500 people.[30] This newly directed focus will explore the underlying causes of incidents to identify potential issues of noncompliance industry-wide. The effort also aims to better understand systemic issues among HIPAA-regulated entities and provide insight that can enhance security programs.[31]

Assessing the Impact

Overall

Maryland ranks 10th among states with the largest number of records compromised from 2013 to 2016 (Table 2). During this period, rate of growth for records compromised increased over 200 percent[32] as compared to a 34 percent[33] rate of growth for the nation. The number of breach occurrences increased twofold[34]. Three breaches stand out from 2014 to 2016, two involved health plans and the other a health care provider. Each of these breaches involved well over 100K records and, together, account for nearly 94 percent of all records compromised in the State.[35] These events elevated Maryland's ranking for total records compromised from 22nd in 2013 to among the top six worst performing states for 2014, 2015, and 2016 (Table 2). Impact for the remaining breaches in Maryland during this same time period consist of seven with fewer than 1K records[36], ten with a range of 1K to 10K records, and three between 10K and 50K records. Nationally, breaches with an impact of fewer than 10K records occurred more frequently, accounting for about 79 percent of all breaches from 2013 through 2016.

Maryland is among 11 states that experienced at least one breach that compromised 1 million records or more between 2013 and 2016.[37] A total of 13 breaches resulted in compromised records exceeding 1

[27] See n. 13, *Supra*.

[28] Median denotes the middle value in a range of numbers.

[29] Total records compromised (#): Hacking/IT (1,145,599); Theft (59,942); Unauthorized/Access Disclosure (876,865).

[30] U.S. Department of Health and Human Services, *OCR Announces Initiative to More Widely Investigate Breaches Affecting Fewer than 500 Individuals,* August 2016. Available at: healthlawpolicymatters.com/wp-content/uploads/sites/8/2016/08/OCR-Announcement-8-18-16.pdf.

[31] This shift in focus follows a recommendation from the Department of Health & Human Services Office of Inspector General in September 2015 to implement a permanent HIPAA compliance audit program that includes and standardizes investigations of smaller health breaches.

[32] Maryland Records compromised (#): 2013 (16,658); 2014 (273,719); 2015 (1,131,380); 2016 (661,269). Compound Annual Growth Rate: 241 percent.

[33] Nation Records compromised (#): 2013 (6,950,118); 2014 (12,737,973); 2015 (113,267,174); 2016 (16,626,349). Compound Annual Growth Rate: 34 percent.

[34] Maryland breaches went from three in 2013 to six in 2014; number of occurrences remained, for the most part, consistent each year thereafter. Breach occurrences (#): 2013 (3); 2014 (6); 2015 (8); 2016 (6); Total 2013-2016 (23).

[35] 2014: Indian Health Service (health plan) – 214,000 records; 2015: CareFirst BlueCross BlueShield (health plan) – 1,100,000 records; and 2016: Bon Secours Health System (health care provider) – 651,971 records. Indian Health Service Plan is a federal program for approximately 2.2M American Indians and Alaska Natives belonging to 567 federally recognized tribes in 36 states. For more information, visit: www.ihs.gov/aboutihs/.

[36] These seven occurrences had at least 500 records compromised, in accordance with OCR reporting requirements.

[37] Other states include: Arizona, California, Florida, Illinois, Indiana, Montana, New York, Texas, Tennessee, and Washington.

million. These breaches occurred in five health plans, four health care providers, and four business associates. New York and Indiana each experienced two such breaches. The breaches in Indiana included the Anthem attack that compromised over 78 million records, and is thought to have served as a strong catalyst for health care systems' increased efforts to enhance security protections consistent with other business sectors.[38] The impact resulting from the Anthem breach accounts for over 50 percent of all records compromised nationally during this time period. Montana, ranking 13th, stands out given its much smaller population size.[39] Certain states experienced fewer compromised records (<25K per breach), such as Michigan and Colorado, but reported more breaches than Maryland. These results illustrate that breaches occur indiscriminately with varying intensity. The small-scale breaches also demonstrate the importance for health care organizations of all sizes to improve security measures and reduce vulnerabilities.

Comparable States

Maryland ranks 3rd for the number of records compromised relative to six comparable states (Table 3).[40] While these six comparison states and Maryland experienced, on average, about 24 breaches during this time period, differences exist in the breadth of records compromised. Colorado, Connecticut, and Missouri experienced an impact that was much less (<50K records per breach), as compared to Arizona, Indiana, Maryland, and New Jersey, which reported several breaches close to or exceeding 1M records. Similar to Maryland, four of these states (Arizona, Connecticut, Indiana, and New Jersey) had at least two breaches each that account for more than 80 percent of all records compromised.[41] Among most of these states, hacking/IT incidents that exposed vulnerabilities in network servers and electronic medical records (EMR) were most often reported as the location of a breach. New Jersey stands out with its largest breaches reported as resulting from laptop and email thefts.

[38] Bankinfo Security, *Anthem Breach Sounds a Healthcare Alarm,* February 2015. Available at: bankinfosecurity.com/anthem-follow-up-a-7878.

[39] Montana, with an estimated population of 1M, experienced a total of seven breaches. A 2014 breach reported by the Montana Department of Public Health & Human Services accounts for the majority (98 percent) of all records compromised from 2013 to 2016.

[40] Comparable states were selected based on data from The Henry J. Kaiser Family Foundation according to population size, total number of providers, and number of hospitals. For more information, visit: kff.org/state-category/providers-service-use/.

[41] See Appendix B for more information on breaches less than and greater 10K records.

Table 2: State Ranking by Total Records Compromised
2013-2016

State	2013-2016			2013	2014	2015	2016	State	2013-2016			2013	2014	2015	2016
	Count	Records	Rank	Rank					Count	Records	Rank	Rank			
IN	39	83,704,657	1	4	15	1	10	MI	25	112,215	27	30	25	19	18
NY	72	14,182,939	2	5	8	3	2	AR	14	104,187	28	35	43	30	13
WA	28	11,636,002	3	7	26	2	7	MS	9	101,986	29	44	36	25	14
CA	142	7,604,892	4	2	5	4	4	UT	9	89,272	30	34	21	44	19
TN	32	5,091,814	5	8	1	11	23	CO	24	82,373	31	31	19	34	32
AZ	24	4,618,277	6	27	14	31	1	LA	12	78,481	32	17	35	23	31
IL	62	4,426,764	7	1	7	16	21	CT	13	72,827	33	41	41	33	16
TX	94	3,694,631	8	3	2	8	9	NV	7	71,578	34	15	30	24	45
FL	90	3,165,787	9	6	10	14	3	KS	7	70,634	35	45	29	32	17
MD	23	2,083,026	10	22	6	5	6	NM	11	49,370	36	24	32	42	26
GA	40	1,799,561	11	12	20	6	5	OK	10	47,386	37	45	31	20	41
NJ	20	1,416,183	12	23	3	37	11	NE	6	45,356	38	33	43	39	22
MT	7	1,107,823	13	39	4	28	24	IA	9	35,515	39	28	37	44	30
VA	18	876,521	14	21	11	7	20	WY	5	31,361	40	16	40	44	44
OH	44	587,246	15	18	28	18	8	RI	4	31,100	41	37	43	29	34
MN	31	272,380	16	25	18	9	33	DE	3	30,435	42	45	39	44	25
PA	40	262,268	17	13	16	13	15	DC	5	26,814	43	45	38	26	42
OR	20	256,354	18	32	17	10	38	SD	5	23,779	44	29	43	27	46
NC	31	243,371	19	11	9	21	27	AK	3	16,828	45	40	43	43	37
MO	25	187,442	20	10	33	22	12	NH	2	16,208	46	45	42	44	35
MA	26	132,764	21	14	24	17	28	HI	2	12,988	47	45	43	35	39
PR	9	126,881	22	19	12	44	46	ND	2	12,000	48	26	43	44	46
KY	19	123,860	23	43	27	12	40	ID	1	6,900	49	45	34	44	46
SC	14	122,280	24	20	22	15	43	ME	3	3,274	50	38	43	41	46
AL	17	114,581	25	36	13	36	29	VT	2	2,550	51	42	43	38	46
WI	12	113,551	26	9	23	40	36	WV	1	-	52	45	43	44	46

Notes: Count represents the number of breach occurrences; strikethrough (-) represents unknown data.

Table 3: Comparable States Ranking by Total Records Compromised
2013-2016

Comparative Ranking	State	Count	Records	Overall Rank (Table 2)
1	IN	37	83,704,657	1
2	AZ	24	4,618,277	6
3	MD	23	2,083,026	10
4	NJ	20	1,416,183	12
5	MO	25	187,442	20
6	CO	24	82,373	31
7	CT	13	72,827	33

Examining Breach Location

Occurrences

There are similarities and variation in the reported location of breached information in Maryland and the nation. Generally, Maryland has experienced more noticeable fluctuations in breach locations. Laptops were reported most in 2013 followed by email. Laptops continued to account for about a third of breaches in 2014 and began to decline in 2015; laptops were not cited as a breach location in 2016. Email resurfaced in 2015 and 2016 in fewer than a quarter of breaches. Nationally, laptops were the leading breach location in 2013 but then declined, similar to Maryland. Desktop computers were not reported as a breach location in Maryland until 2016, when they exceeded the nation by more than double (Figures 2 and 3). While EMR has consistently appeared year after year as a location for breaches nationally, it did not emerge in Maryland until 2015. Records compromised for EMR has been minimal as compared to network servers, which has been the dominant location compromising the vast majority of records in 2015 and 2016.[42]

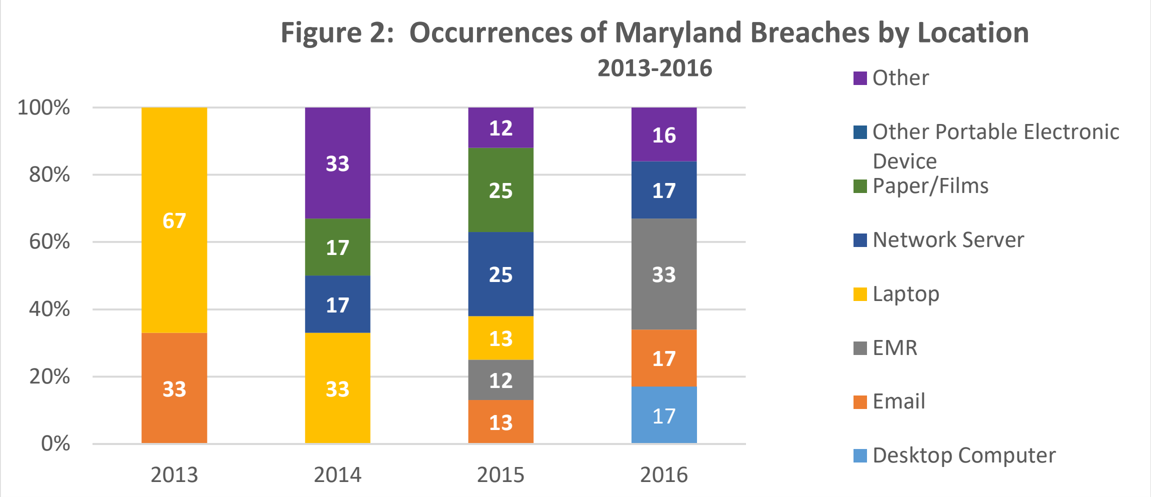
Figure 2: Occurrences of Maryland Breaches by Location
2013-2016

Notes: More than one breach location was reported for approximately 16 percent of breaches; other is selected by a CE or BA reporting a breach when no other location option applies.

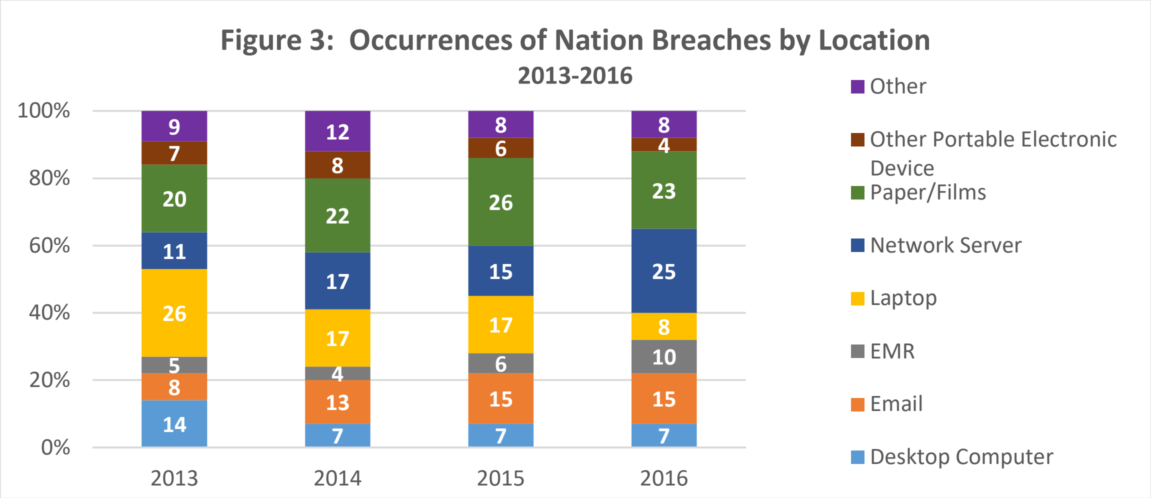
Figure 3: Occurrences of Nation Breaches by Location
2013-2016

Notes: More than one breach location was reported for approximately 20 percent of breaches; the location for a portion of breaches is unknown and not represented in this figure.

[42] See Appendix C for actual number of occurrences by breach location for Maryland and the nation.

Records Compromised

Quantifying records compromised based on breach location provides perspective about specific areas of vulnerability. In 2013, laptops accounted for over half (54 percent) of records compromised in Maryland; email was the location for the remaining records compromised (46 percent). Though occurrences in Maryland attributed to laptops as the breach location decreased by half in 2014, impact more than doubled with laptops being the primary location for almost all records compromised (94 percent). Nationally, a shift occurred in 2014 when email and network servers were identified as the location for over 75 percent of records compromised. In 2015, network servers became the predominant breach location for Maryland and amplified for the nation, accounting for about 95 percent of records compromised. This is largely due to massive breaches reported by health plans.[43] Network servers remained the trend for Maryland in 2016 while the nation experienced a slight decrease just under 80 percent (Table 4).[44] Breaches from network servers are mainly attributed to hacking/IT incidents.[45] Network intrusion can occur through multiple points of entry (e.g., a phishing email that contains the link to a spoofed webpage tricking users to disclose their system credentials).

Table 4: Compromised Records by Breach Location
2013-2016
%

Location of Breach	2013		2014		2015		2016	
	MD	Nation	MD	Nation	MD	Nation	MD	Nation
Desktop Computer	0	63	0	2	0	<1	<1	<1
Email	46	1	0	20	3	<1	<1	7
EMR	0	<1	0	1	<1	3	<1	3
Laptop	54	15	94	11	<1	<1	0	5
Network Server	0	5	4	57	97	95	99	79
Paper/Films	0	8	<1	5	<1	<1	0	5
Other Portable Electronic Device	0	2	0	1	0	<1	0	<1
Other	0	6	2	3	<1	<1	1	1

Protecting Network Assets

In addition to network servers, other connected network assets exist where electronic PHI resides, such as medical devices, tablets, mobile phones, email, and EMR systems. Safeguards most often implemented by health care organizations include server antivirus and malware prevention, two-factor authentication, encryption of data at rest, vulnerability testing, and tamper-proofing of administrative settings. Upgrading operating systems is another way to enhance network protections. For instance, Microsoft Windows 10 Enterprise Operating System meets many technical and administrative safeguards required by HIPAA. Windows 10 aims to improve security by including additional protections pertaining to user identities, information, and devices.[46, 47]

[43] See n. 2, *Supra*.
[44] See Appendix D for number of records compromised by location of breach for Maryland and the nation.
[45] Nearly 64 percent of breaches citing network server as the location are the result of a hacking incident.
[46] Microsoft Windows 10 is designed to protect user identity, device, and data. For more information, visit: www.hipaaone.com/wp-content/uploads/2017/05/HIPAA-and-Win-10-FINAL-Updated-Appendix.pdf.
[47] For more information, visit: www.microsoft.com/en-us/windowsforbusiness/windows-security.

A Preliminary View of 2017

Preliminary data for 2017[48] suggests that breach trends nationally remain on par with previous years. The recent surge in hacking/IT continues to account for a sizeable portion of all breaches (~42 percent) and records compromised (~70 percent). Unauthorized access/disclosure is the second most common breach type reported (~36 percent) though the impact of records compromised is much smaller (~10 percent). Network servers have been cited most frequently as the breach location for hacking/IT. Half of breaches reported so far in Maryland involve hacking/IT, citing network server in addition to email or EMR as the breach location. Health care providers remain the most vulnerable, reporting the majority of breaches (~80 percent), including all but one of eight reported breaches in Maryland.[49] While Maryland experienced an increase in reported breaches (from six in 2016 to eight in 2017[50]), the number of records compromised has been substantially less. Maryland breaches reported so far in 2017 have compromised about 55K records in total as compared to previous years when the impact was closer to or exceeded 1M records. As of November 2017, Maryland ranks 16th for total records compromised, descending about 10 spots from its rank in 2016.

Conclusion

The health care industry is struggling to acclimate to the complex world of cybersecurity. HIPAA-regulated entities are cognizant of cyber threats, but need to further improve security to keep pace with evolving threats. Among these entities, health care providers are the most challenged in meeting increased security demands and, in Maryland, are making incremental strides to improve cybersecurity preparedness. As the health care industry continues its transition towards integrated care delivery, greater sharing of electronic patient information has been judged as a prerequisite to achieving the goals of healthier people, better care, and smarter spending. Increased use and integration of electronic systems requires adequate planning of security controls to ensure confidentiality, integrity, and availability of PHI at the point of care. Continuous improvement of cybersecurity is critical in reducing the risk and magnitude of breaches. Such improvement will involve the deployment of preventative measures, while also preparing response and recovery protocols to activate when a security incident is suspected. HIPAA-regulated entities throughout Maryland are encouraged to strengthen cybersecurity protocols, foster user awareness and education about cybersecurity best practices, and keep breach remediation teams well-trained and ready for quick deployment.

[48] Includes breaches investigated and closed and those still under investigation as of November 2017.

[49] Maryland reported breaches by CE Type (#): Health care providers (7); BA (1).

[50] Note: Six of the eight breaches reported are still under investigation.

Appendix A: OCR Definitions

Breach Type

- Hacking/IT: if electronic PHI was impermissibly accessed through technical intrusions (including by malware or directed hacking) to the CE's or BA's systems, servers, desktops, laptops, mobile devices, etc.
- Unauthorized Access/Disclosure: if no other category applies. For example, select for a misdirected mailing or other communication.
- Theft: if equipment housing electronic PHI (servers, desktops, laptops, back-up tapes, thumb-drives, mobile devices, copiers, or other hardware) or if paper records were stolen, or if you believe they were stolen. If electronic PHI was stolen as a result of a technical intrusion, choose "Hacking/IT Incident".

Breach Location

- Desktop computer: stationary computer
- EMR: PHI printed or viewed directly from an electronic health or medical record
- Email: PHI was improperly accessed or disclosed by email
- Laptop: portable computer
- Network server: PHI was improperly accessed or disclosed through a network server
- Other portable electronic device: any portable electronic device (e.g., smartphone, tablet, external storage device) that is not a laptop
- Paper/films: paper or other hard copy of PHI (e.g., misdirected mailings or faxes and missing or stolen x-rays)
- Other: if no other option applies (e.g., PHI was impermissibly disclosed orally)

Appendix B: Maryland and Comparable States

The tables below detail number (or count) of breach occurrences and records compromised for Maryland and comparable states based on an impact that was less than and greater than 10K records.

Comparable States Breaches < 10,000 Records
2013-2016

State	2013		2014		2015		2016		Total	
	Count	Records	Count	Records	Count	Records	Count	Records	Count	Records
AZ	5	10,914	4	7,147	4	6,854	6	7,452	19	32,367
CO	6	7,722	5	13,606	3	2,957	7	18,871	21	43,156
CT	1	1,382	2	1,385	4	5,115	4	5,600	11	13,482
IN	8	21,879	4	4,975	4	7,066	10	38,432	26	72,352
MD	3	16,658	3	6,240	6	6,413	5	9,298	17	38,609
MO	8	18,465	3	7,989	4	13,354	4	16,505	19	5,6313
NJ	3	13,425	3	4,824	2	2,620	4	12,494	12	33,363

Comparable States Breaches ≥ 10,000 Records
2013-2016

State	2013		2014		2015		2016		Total	
	Count	Records	Count	Records	Count	Records	Count	Records	Count	Records
AZ	0	0	2	69,084	0	0	3	4,516,826	**5**	4,585,910
CO	0	0	3	39,217	0	0	0	0	**3**	39,217
CT	0	0	0	0	0	0	2	59,345	**2**	59,345
IN	2	197,883	1	63,325	6	83,152,355	2	218,742	**11**	83,632,305
MD	0	0	3	267,479	2	1,124,967	1	651,971	**6**	2,044,417
MO	2	35,461	0	0	1	12,500	3	83,168	**6**	131,129
NJ	0	0	4	1,253,665	0	0	4	129,155	**8**	1,382,820

Appendix C: Occurrences by Breach Location

The table below depicts the number of occurrences by breach location for Maryland and the Nation.

Breach Location
Occurrences
2013-2016

Location of Breach	2013		2014		2015		2016	
	MD	Nation	MD	Nation	MD	Nation	MD	Nation
Desktop Computer	0	37	0	21	0	20	1	22
Email	1	22	0	37	1	40	1	49
EMR	0	14	0	13	1	17	2	31
Laptop	2	71	2	51	1	45	0	26
Network Server	0	30	1	49	2	41	1	82
Paper/ Films	0	53	1	65	2	69	0	74
Other Portable Electronic Device	0	20	0	24	0	16	0	13
Other	0	24	2	34	1	21	1	28
Total	3	271	6	294	8	269	6	325

Appendix D: Records Compromised by Breach Location

The table below illustrates the number of records compromised by breach location for Maryland and the nation.

Breach Location
Records Compromised
2013-2016

Location of Breach	2013		2014		2015		2016		Total	
	MD	Nation	MD	Nation	MD	Nation	MD	Nation	MD	Nation
Desktop Computer	0	4,336,603	0	305,840	0	204,209	860	91,090	860	4,937,742
Email	7,606	70,373	0	2,519,625	24,967	674,043	907	1,013,787	33,480	4,277,828
EMR	0	40,196	0	117,909	1,029	3,938,991	2,700	433,862	3,729	4,530,958
Laptop	9,052	1,030,485	256,713	1,391,012	571	425,781	0	812,946	266,336	3,660,224
Network Server	0	320,127	10,766	7,258,653	1,101,475	107,252,466	651,971	13,175,265	1,764,212	128,006,511
Paper/ Films	0	575,076	620	606,523	2,838	232,552	0	839,865	3,458	2,254,016
Other Portable Electronic Device	0	154,877	0	195,494	0	217,766	0	23,154	0	591,291
Other	0	422,381	5,620	342,917	500	321,366	4,831	236,380	10,951	1,323,044
Total	16,658	6,950,118	273,719	12,737,973	1,131,380	113,267,174	661,269	16,626,349	2,083,026	149,581,614

David Sharp, Ph.D.

Director

Center for Health Information Technology and Innovative Care Delivery

MARYLAND
HEALTH CARE
COMMISSION

4160 Patterson Avenue

Baltimore, MD 21215

410-764-3460

www.mhcc.maryland.gov