

Health Care Data Breaches: 2017 Findings



September 2018

Robert E. Moffit, PhD, Chair
Ben Steffen, Executive Director

Maryland Health Care Commission



Robert E. Moffit, PhD, Chair
Senior Fellow, Health Policy Studies
Heritage Foundation

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

Marcia Boyle
Founder
Immune Deficiency Foundation

Elizabeth A. Hafey, Esq.
Associate
Miles & Stockbridge P.C.

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

Jason C. McCarthy
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

Candice A. Peters, MD
Physical Medicine and Rehabilitation in
Private Practice

Martha G. Rymer
Rymer & Associates, P.A.

Randolph S. Sergent, Esq.
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

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

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

Table of Contents

Introduction	4
Approach and Limitations	5
Overview of 2017 Findings	6
A Preliminary View of 2018	11
OCR Audits	12
Summary	12
Appendix A	13
Appendix B	14
Appendix C	15
Appendix D	16
Appendix E	17
Appendix F	18
Appendix G	19

Introduction

The health care industry remains a lucrative target for malicious attacks. Health care organizations face persistent challenges in safeguarding consumer information. In 2017, reported breaches increased for the nation and Maryland, while number of records compromised decreased considerably. Breaches affecting more than one million records¹ have become less frequent; however, a single breach occurrence can still render disastrous results for health care organizations and consumers. Since 2015, reported breaches for hacking/IT have grown faster than other breach types² and generally account for the majority of all records compromised.

Malicious attacks seize protected health information (PHI)³, which often times is extorted or held ransom in exchange for payment.⁴ Ransomware, the most common type of malware today, accounts for 85 percent of all malware targeting the health care sector.^{5,6} Attackers typically take advantage (exploit) weaknesses in elemental cybersecurity measures, increasing risk of a breach for health care organizations.⁷ Common vulnerabilities exploited by human and technical weaknesses include outdated security patches or software updates⁸, weak passwords, and uncredentialed access⁹ to information systems that contain electronic PHI.¹⁰

The Equifax breach and the WannaCry virus (a type of ransomware) broke records in 2017 and highlight the importance of cybersecurity basics across all industries. In the case of Equifax, an attacker took advantage of a vulnerability where a software update (or patch) was made available two months prior (in March) but was not installed until May, upon discovery of the breach.¹¹ Nearly 150 million records were compromised spanning residents across the United States, Europe, and Canada.¹² The WannaCry virus created a ransomware epidemic by infiltrating Microsoft operating systems through a known vulnerability in older versions of its Windows software (particularly, Windows XP).¹³ The impact of the WannaCry virus extended to more than 150 countries; the Department of Homeland Security estimates infection in the United States was minimal due to early warnings from news reports and alerts.

¹ Hacking/IT breaches in 2015 brought about some of the largest breaches in history involving health plans; Nation: Anthem BlueCross (80M records); Premera BlueCross (11M records); Excellus BlueCross BlueShield (10M records). Maryland: CareFirst BlueCross BlueShield (1.1M records).

² Breach types include: hacking/IT, improper disposal, loss, theft, and unauthorized access/disclosure. For more information, visit: ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

³ 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 business associate.

⁴ A report conducted by Beazley, a cybersecurity insurance company, analyzed more than 2,600 data breaches reported in 2017 and found that 45 percent of all ransomware attacks occurred in the health care sector. For more information:

beazley.com/documents/Whitepapers/201802-beazley-breach-briefing.pdf.

⁵ Verizon, *2018 Data Breach Investigations report*, March 2018. Available at:

verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf.

⁶ 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 to gain system access by manipulating individuals into divulging confidential information.

⁷ InfoWorld, *Annual Verizon security report says sloppiness causes most data breaches*, April 2017. Available at:

infoworld.com/article/3193028/security/annual-verizon-security-report-says-sloppiness-causes-most-data-breaches.html.

⁸ A report conducted by the Ponemon Institute revealed that 57 percent of respondents experienced a breach due to a patch vulnerability.

For more information: hipaajournal.com/study-reveals-poor-patching-practices-in-healthcare/.

⁹ Nearly half of hacking incidents involve theft or misuse of credentials. For more information: calyptix.com/hipaa/top-5-causes-of-data-breaches-in-healthcare/.

¹⁰ See n. 5, *Supra*.

¹¹ Wired, *Equifax officially has no excuse*, September 2017. Available at: wired.com/story/equifax-breach-no-excuse/.

¹² The Washington Post, *Equifax's massive 2017 data breach keeps getting worse*, March 2018. Available at: [washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/?utm_term=.26748abbf432](https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/?utm_term=.26748abbf432).

¹³ Forbes, *How WannaCry Went From A Windows Bug to An International Incident*, May 2017. Available at: forbes.com/sites/leemathews/2017/05/16/wannacry-ransomware-ms17-010/#7692ad8e2609.

Health care organizations evaluate risks and determine which risks they are willing to accept. When a risk is deemed too severe, remediation efforts are enacted. Knowing when to act is essential to a risk management strategy; equally important is the means to identify root causes and proper implementation of controls to reduce a vulnerability. A key lesson learned from the Equifax breach and WannaCry virus is the importance of robust patch management processes, especially for organizations operating on legacy platforms. Patch management, however, is not the panacea of cybersecurity. Other controls to mitigate risk include implementing multi-factor authentication¹⁴, preventing unauthorized software installations, and removing or blocking unnecessary software and browser plugins (e.g., installing antivirus software and ad-blocking).¹⁵ Cybersecurity experts recommend health care organizations conduct frequent and comprehensive risk assessments to evaluate and build defenses, taking into consideration the latest trends and risks to improve privacy and security controls long-term.¹⁶

Approach and Limitations

The Maryland Health Care Commission (MHCC) analyzed health care data breaches affecting 500 or more individuals that were reported by covered entities (CE)¹⁷ and business associates (BA)¹⁸ in 2017 to the Department of Health & Human Services, Office for Civil Rights (OCR). Data was retrieved from the OCR online portal.¹⁹ This information brief presents a summary of findings from breaches reported in Maryland and the nation and an update on key trends.²⁰

Findings are subject to change based on conclusions from OCR investigations that remain open as of June 2018 (breaches open/closed: Nation 211/148; Maryland 4/4).^{21, 22, 23} Breaches are reported based on where the headquarters of a CE or BA resides. Analysis of breaches by year is based on the submission date of the breach report to OCR and may be different than the breach occurrence date (CEs and BAs have 60 calendar days from discovery to report a breach to OCR). OCR breach data does not always include specifics related to breach origin (e.g., ransomware, phishing, etc.). Reporting organizations select breach type and location on the form used to report a breach. A CE's and BA's perspective about a type of breach may vary among individuals that file the report with OCR.²⁴

¹⁴ Multi-factor authentication is the process of identifying an online user by validating two or more claims presented by the user, including something the user knows, something the user has, and something the user is. The goal is to strengthen security by compensating for weaknesses of one factor (e.g., a password) with supplemental factors (e.g., a key bound to a user's mobile device).

¹⁵ Infosec Institute, *10 Best Practices for Healthcare Security*. Available at: resources.infosecinstitute.com/category/healthcare-information-security/is-best-practices-for-healthcare/10-best-practices-for-healthcare-security/#gref.

¹⁶ Intel, *Improving Healthcare Risk Assessments to Maximize Security Budgets*. Available at: intel.com/content/dam/www/public/us/en/documents/solution-briefs/risk-assessments-maximize-security-budgets-brief.pdf.

¹⁷ CEs include health plans, health care clearinghouses, and health care providers. For more information: hhs.gov/hipaa/for-professionals/breach-notification/index.html.

¹⁸ BAs include entities that create, receive, maintain or transmit PHI on behalf of a CE or another BA.

¹⁹ The portal includes details, including but not limited to, name of involved covered entity (CE), CE type, number of individuals affected, breach submission data, type of breach, and location of breached information. Data for 2017 was accessed from the OCR portal on June 19, 2018. For more information: ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

²⁰ Maryland Health Care Commission, *Health Care Data Breaches: How Maryland Compares*, December 2017. Available at: mhcc.maryland.gov/mhcc/pages/hit/hit_cybersecurity/documents/AllStateBreaches_Final.pdf.

²¹ See Appendix A for list of Maryland Breaches.

²² A total of 40 investigations remain open from breaches reported in 2016; all breaches from prior years have been closed.

²³ In the last three years, less than 10 percent of OCR's breach compliance review investigations were found to have no violation. For more information: hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html.

²⁴ OCR instructs reporting entities to select "unauthorized access/disclosure" as breach type for circumstances where no other category applies.

Overview of 2017 Findings

The health care industry continued to see an increase in breaches with an all-time high of 359 reported in the nation (Table 1), of which 80 percent were by health care providers (Figure 1). Breaches in Maryland have remained fairly consistent over the past few years, up two breaches from the prior year for a total of eight breaches in 2017. Nationally, hacking/IT breaches remain the biggest threat, and for the first time, surpassed all other breach types at 42 percent. Unauthorized access/disclosure accounts for the next largest portion of breaches at 35 percent. This includes insider-wrongdoing, which involved the largest breach reported by a health care provider (Commonwealth Health Corporation) in Kentucky with 697,800 patient billing records.²⁵ An investigation determined the cause was due to inappropriate access (i.e., no work-related reason) by an employee who obtained PHI on an encrypted device.²⁶ In contrast to the increase in the number of reported breaches, the nation and Maryland experienced a sizable decrease in total records compromised (Table 1), a 69 percent decrease from the prior year.

Table 1. Local and National Breaches										
	2014		2015		2016		2017		Total	
	Count	Records	Count	Records	Count	Records	Count	Records	Count	Records
Maryland	6	273,719	8	1,131,380	6	669,919	8	55,961	28	2,130,979
Nation	294	12,285,589	269	113,265,216	326	16,626,349	359	5,138,179	1,248	147,315,333

Note: Count represents the number of reported breaches to OCR; records represent the number of records compromised for reported breaches during the year specified.

Reported Breaches

Reported breaches increased by 33 from the prior year, averaging about one breach per day.²⁷ The average time until breach discovery increased by 32 percent to 308 days as compared to 233 days in 2016. Health care providers continue to report the greatest number of breaches (Nation: 80 percent; Maryland: 88 percent) accounting for all of the top 10 breaches in the nation and all but one in Maryland (Figures 1 and 2).^{28, 29} Ransomware attacks have increased, and some believe breaches resulting from such incidents could be underreported due to fear of reputational harm and loss of public trust.³⁰ Health care organizations face paying ransoms as a way to avoid disruption in access to critical technology required to support care delivery. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Breach Notification Rule established reporting requirements that are detailed on the OCR public website.³¹ Requests from the industry and members of Congress prompted OCR to release guidance in August 2016 highlighting the differences between ransomware and traditional data breaches. This guidance clarifies circumstances when ransomware constitutes a breach.³² OCR issued a reminder about this guidance in May 2017 following the outbreak of the WannaCry virus.

²⁵ Included patients' names, addresses, Social Security numbers, health insurance information, diagnoses, procedure codes and charges for medical services.

²⁶ Protensus, Inc., *Breach Barometer Report: Year in Review, 2017*.

²⁷ This includes breaches that are closed and currently under investigation by OCR.

²⁸ See Appendix B.

²⁹ See Appendix C and D for breakdown in the percentage of reported breaches by CE type and BAs.

³⁰ Healthcare IT News, *Insiders, Hackers Causing Bulk of 2017 Healthcare Data Breaches*, Jessica Davis, Healthcare IT News, August 2017.

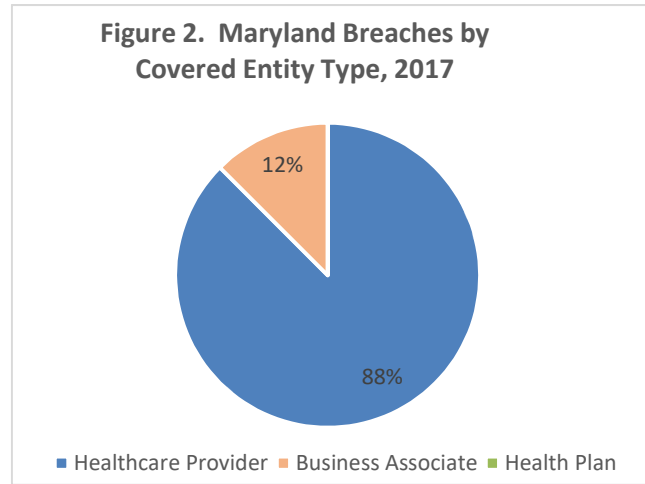
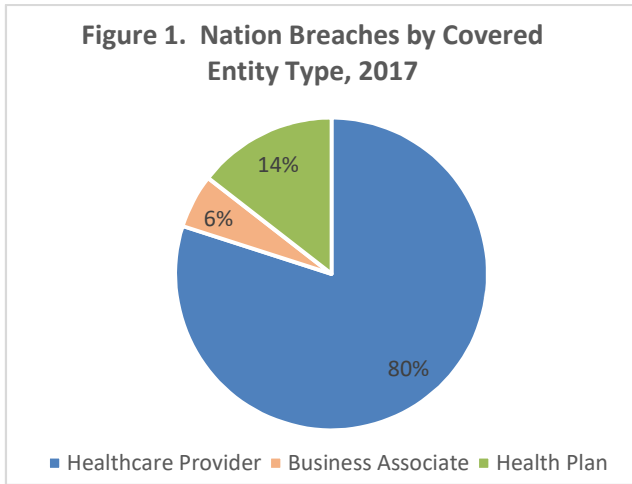
Available at: healthcareitnews.com/news/insiders-hackers-causing-bulk-2017-healthcare-data-breaches.

³¹ HealthcareIT News, *Ransomware rising, but where are all the breach reports?*, March 2017. Available at:

www.healthcareitnews.com/news/ransomware-rising-where-are-all-breach-reports

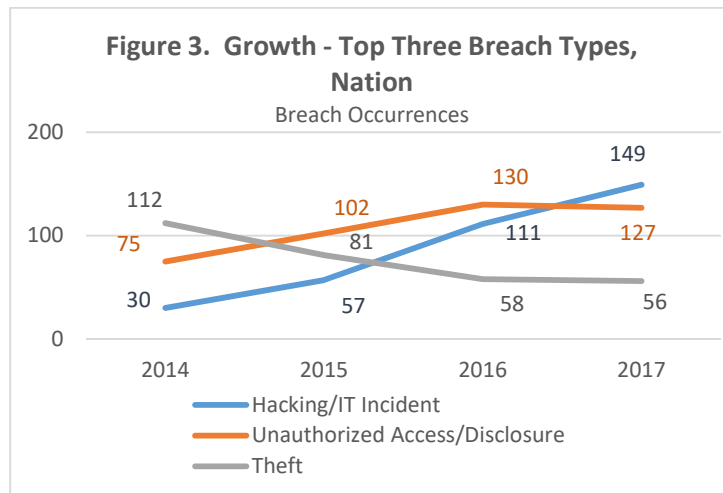
³² Department of Health & Human Services, *Fact Sheet: Ransomware and HIPAA*, July 2016. Available at:

hhs.gov/sites/default/files/RansomwareFactSheet.pdf.



Breach Types

Since 2014, reported hacking/IT breaches have grown at a compound annual growth rate of 71 percent. Hacking/IT breaches were reported most often in 2017 nationally and locally (Figures 3 and 4). There was a decrease of five percent in the nation for total reported breaches for unauthorized access/disclosure compared to the previous year,³³ the first since 2014. Following hacking/IT, unauthorized access/disclosure continues to account for a sizeable portion of breaches in the State. It is estimated that ransomware represents a quarter of all hacking/IT breaches, an increase of 89 percent since 2016.³⁴ Ease in generating mass or targeted phishing e-mails is a key contributor to the increase in ransomware and a major threat to health care organizations, preventing access to information systems by potentially tampering, exploiting, or hindering patient care. Continuous system monitoring to detect abnormal user behavior and employee training to identify suspicious emails are examples of essential components of a risk management strategy.³⁵

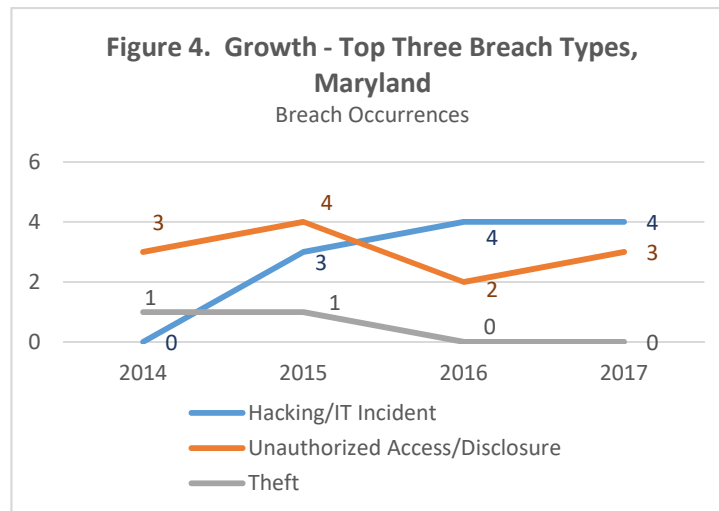


Note: Other breach types occurred (i.e., loss, improper disposal) for a small portion of breaches.

³³ See table 1 for total breaches and records compromised by year.

³⁴ Healthcare Informatics, *Report: Ransomware Attacks Against Healthcare Orgs Increased 89 Percent in 2017*, January 2018. Available at: healthcare-informatics.com/news-item/cybersecurity/report-ransomware-attacks-against-healthcare-orgs-increased-89-percent-2017.

³⁵ SANS Institute, *Healthcare Provider Breaches and Risk Management Road Maps: Results of the SANS Survey on Information Security Practices in the Healthcare Industry*, July 2016. Available at: sans.org/reading-room/whitepapers/hipaa/healthcare-provider-breaches-risk-management-road-maps-results-survey-informati-37105.



Note: Other breach types occurred (i.e., loss, improper disposal) for a small portion of breaches.

Records Compromised

A steep decline in total records compromised occurred in 2017, decreasing from the prior year by as much as 69 percent nationally and 92 percent locally (Figure 5). All breaches affected fewer than one million records, a departure from previous years when several breaches exceeding one million records were reported by select states, including Maryland.³⁶ The majority of records compromised continues to be attributed to hacking/IT breaches, accounting for 95 percent of records for Maryland and 68 percent of all records across the nation.^{37,38} Total records compromised in Maryland decreased relative to other states. Maryland now ranks 20th among all states for total records compromised, improving 14 spots since 2016.³⁹ The total records compromised and number of reported breaches vary among states with similar populations to Maryland (Table 2).⁴⁰ Among six comparable states,⁴¹ Maryland ranks 4th highest among the six states for records compromised. Maryland's experience most closely resembles that of New Jersey and Arizona.

³⁶ Number of breaches that compromised over one million records: 2013 (1); 2014 (3); 2015 (6); 2016 (3).

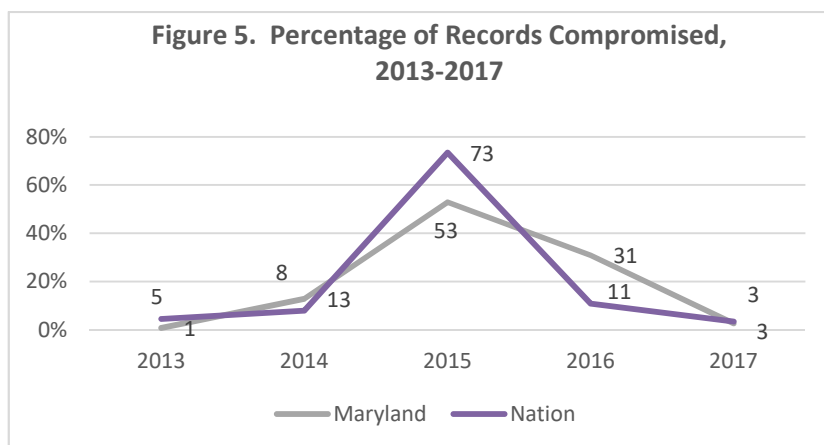
³⁷ Refer to MHCC's December 2017 report *Health Care Data Breaches: How Maryland Compares* for historical information. Available at: mhcc.maryland.gov/mhcc/pages/hit/hit_cybersecurity/documents/AllStateBreaches_Final.pdf.

³⁸ Hacking/IT breaches account for nine out of the 10 largest breaches reported to OCR in 2017, see Appendix B.

³⁹ Maryland breaches reported less than 60,000 records total, a significant decrease from well over 600,000 records in 2016.

⁴⁰ See Appendix E for the top ten states for records compromised.

⁴¹ 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: www.kff.org/state-category/providers-service-use/.



Notes: The graph depicts the distribution of records compromised by year. Breaches in 2015 compromised the greatest number of records to date in Maryland and the nation, including Anthem BlueCross (78.8M records), Premera BlueCross (11M records), Excellus BlueCross BlueShield (10M records), and CareFirst BlueCross BlueShield (1.1M records). Nation records compromised (#): 2013 (7,022,786); 2014 (12,285,589); 2015 (113,265,216); 2016 (16,626,349); 2017 (5,138,179). Maryland records compromised (#): 2013 (23,085); 2014 (273,719); 2015 (1,131,380); 2016 (669,919); 2017 (55,961).

Table 2. Comparable States Ranking by Records Compromised, 2017			
Comparative Ranking	State (Breach Occurrences)	Records Compromised	Overall Rank
1	IN (9)	176,272	7
2	MO (12)	140,389	11
3	CO (12)	65,982	17
4	MD (8)	55,961	20
5	NJ (8)	46,098	21
6	AZ (8)	35,339	24
7	CT (7)	27,844	28

Breach Location

Breaches citing email as the location increased the most, by ten percent nationally and 33 percent locally (Tables 3 and 4). e-Mail was cited half of the time in Maryland followed by electronic medical record (EMR)⁴² in conjunction with network server. Nationally, network server is the leading breach location. Consistent with prior years, the nation reports paper/films about 20 percent of the time as compared to Maryland where it has not been reported since 2015.

Maryland breaches citing EMR/network server account for nearly two-thirds of records compromised, a decrease from 2016 when network server alone accounted for the vast majority (97 percent) of records compromised. e-Mail accounts for the remaining third. Network server is the location for more than half of records compromised in the nation, a decrease of about 20 percent from the prior year.

⁴² The OCR breach portal utilizes the term EMR. Though sometimes used interchangeably, EMR typically refers to a digital version of a patient's paper chart, while an electronic health record refers to a system that is built to share patient information with the patient's entire clinical care team, within and beyond the organization.

Desktop computer, e-mail, and other portable electronic devices experienced increases in records compromised for the nation by about ten percent (Table 3).

Table 3. Maryland Breaches by Location, 2016-2017				
%				
Breach Location(s) Cited	2016		2017	
	Occurrences N=6	Records N=669,919	Occurrences N=8	Records N=55,961
Desktop Computer	17	1	0	0
Desktop Computer/ EMR	17	<1	0	0
EMR	17	<1	12.5	<1
EMR/ Network Server	0	0	25	63
e-Mail	17	<1	50	35
Network Server	17	97	0	0
Other Portable Electronic Device	0	0	12.5	1
Other	17	1	0	0

Table 4. National Breaches by Location, 2016-2017				
%				
Breach Location Cited	2016		2017	
	Occurrences N=326	Records N=16,640,090	Occurrences N=359	Records N=5,138,179
Desktop Computer	8	1	9	13
e-Mail	15	6	25	14
EMR	11	3	13	5
Laptop	9	5	9	4
Network Server	30	80	31	59
Paper/Films	24	6	20	4
Other Portable Electronic Device	6	<1	7	17
Other	10	32	8	3

Notes: CEs and BAs reporting a breach self-select the breach location(s). Multiple breach locations (up to eight locations) were selected for approximately 11 percent of national breaches; these instances are demonstrated as distinct occurrences within the table and thus the percentages do not equal 100 percent. Other is selected by a CE or BA reporting a breach when no other location option applies. The location for a portion of breaches is unknown and not represented in this table.

A Preliminary View of 2018

Reported breaches thus far in 2018⁴³ suggest prior year trends will continue in the current year. Nationally, hacking/IT breaches and unauthorized access/disclosure both account for around 39 percent of occurrences. Hacking/IT breaches account for 71 percent of all occurrences in Maryland. The majority of records compromised is attributed to hacking/IT breaches (Nation: 62 percent; Maryland: 95 percent) (Table 5). An estimated increase of about 17 percent is projected for number of records compromised in 2018.⁴⁴

Table 5. Maryland and Nation Breaches		
As of August 2018		
	Reported Breaches	Records Compromised
Maryland	7	587,022
Nation	221	4,692,427

Note: Count represents the number of reported breaches to OCR; records represent the number of records compromised.

In Maryland, the less than 60,000 records compromised in 2017 has increased tenfold through August 2018. This increase has pushed Maryland's rank from 20th in 2017 to 3rd as of August 2018 (Table 6).⁴⁵ A hacking/IT breach at a Baltimore health system that lead to the disclosure of over a half million records⁴⁶ accounts for 92 percent of all records compromised in Maryland in 2018 (Table 6).

Table 6. Top 5 States					
As of August 2018					
Rank	State	Number of Breaches	Rank	State	Number of Records Compromised
1	CA	27	1	CA	794,164
2	TX	14	2	TN	610,399
3	MA	13	3	MD	587,022
4	IL	12	4	NY	485,982
5	FL	11	5	MO	460,259

⁴³ Preliminary data include breaches investigated and closed and those still under investigation from January 2018 to August 2018.

⁴⁴ Estimate is based on preliminary data and is subject to change.

⁴⁵ See Appendix F for a list of 2018 Maryland breaches.

⁴⁶ LifeBridge Health, Inc. (538,127).

OCR Audits

Phase 2 of the OCR Audit Program (Phase 2)⁴⁷ shifted focus to smaller breaches affecting less than 500 records that mostly involved health care providers (>90 percent).^{48, 49} The goal is to identify common causes of breaches and to better understand HIPAA compliance challenges. OCR's focus is largely centered on type of PHI exposed or stolen, breaches involving hacking/IT, and instances where numerous breach reports from a CE or BA suggest similarities.⁵⁰ Preliminary results suggest that compliance with HIPAA Privacy, Security and Breach Notification standards is largely inadequate, with over 94 percent failing to demonstrate appropriate risk management plans.⁵¹ Findings will be used to develop guidance for enhanced industry-wide risk monitoring and breach prevention practices.

Summary

Hacking continues to increase in sophistication, with new variants of ransomware emerging daily. While larger health care organizations are becoming more secure, in part to due implementation of more robust privacy and security controls, smaller organizations continue to struggle. Threats will likely continue to grow in complexity and the burden of experiencing a breach is becoming increasingly costly.⁵² Investments in risk assessments and cybersecurity protections will continue to increase as chief executive involvement in cybersecurity risk management increases. Budget and staffing pose practical concerns for most health care organizations in determining the level of information security investment.

A growing number of states are enacting legislation that builds on existing federal breach notification requirements due to increased threats and exposure of PHI. The Maryland Personal Information Protection Act was amended by the General Assembly in April 2018 and will become effective on October 1, 2018.⁵³ The law now includes health information as defined by HIPAA. It also expands the definition of a breach, and provides a timeline for breach notification, among other things. Increasingly, states and health care organizations are taking the mindset that a breach is inevitable. Sound information security planning and risk management is essential to minimizing the impact on consumers and health care organizations.

⁴⁷ In phase 2 of the audit, OCR conducted desk audits to evaluate the implementation of policies and procedures adopted by covered entities to comply with specific requirements of the Privacy, Security and Breach Notification Rules. For more information: lanepowell.com/Our-Insights/110801/Increased-Ransomware-Attacks-and-Phase-2-HIPAA-Audits-Two-Closely-Related-Issues-for-Long-Term-Care-Providers.

⁴⁸ Information on data breaches affecting fewer than 500 individuals is not made publicly available and is not included in this information brief.

⁴⁹ Healthcare informatics, *Former OCR Advisor on HIPAA Compliance and Data Breaches: "This is a Management Problem, Not a User Problem"*, April 2017. Available at: healthcare-informatics.com/article/cybersecurity/former-ocr-advisor-hipaa-compliance-and-data-breaches-management-problem-not.

⁵⁰ Healthcare informatics, *OCR Announces Initiative to Focus Investigations on Smaller Data Breaches*, August 2016. Available at: healthcare-informatics.com/news-item/cybersecurity/ocr-announces-initiative-focus-investigations-smaller-data-breaches.

⁵¹ OCR conducted 207 desk audits (CEs: 166; BAs: 41). For more information: cynergistek.com/blog/ocr-desk-audits-preliminary-results/.

⁵² Coker Group, *Healthcare Cybersecurity Threats and Trends for 2018*, June 2018. Available at: cokergroup.com/healthcare-cybersecurity-threats-and-trends-for-2018/.

⁵³ Maryland General Assembly, *Maryland Personal Information Protection Act – Security Breach Notification Requirements – Modifications*, April 2018. Available at: mgaleg.maryland.gov/2018RS/fnotes/bil_0004/hb1584.pdf.

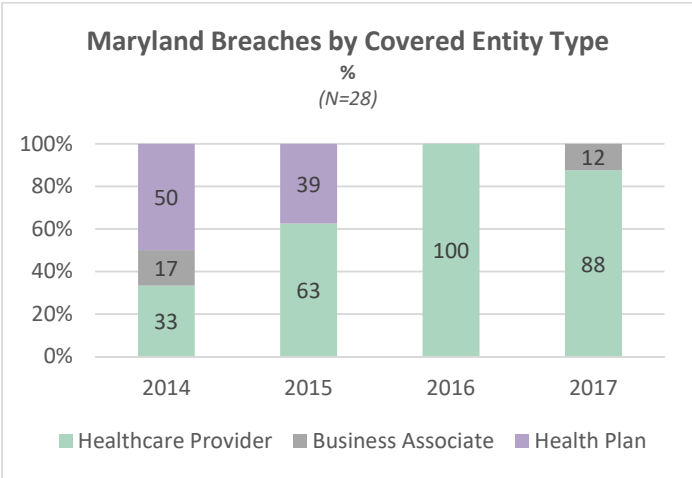
Appendix A

All Maryland Breaches 2017			
Organization	Records Compromised	Type of Breach	Covered Entity Type
Sport and Spine Rehab	31,120	Hacking/IT Incident	Health Care Provider
Chase Brexton Health Care	16,562	Hacking/IT Incident	Health Care Provider
Capital Nephrology	4,000	Hacking/IT Incident	Health Care Provider
University of Maryland Orthopaedic Associates, P.A.	1,320	Hacking/IT Incident	Health Care Provider
Associated Catholic Charities Incorporated	1,145	Unauthorized Access/Disclosure	Health Care Provider
The Union Labor Life Insurance Company	664	Unauthorized Access/Disclosure	Business Associate
Complete Wellness	600	Loss	Health Care Provider
The Affiliated Sante Group	550	Unauthorized Access/Disclosure	Health Care Provider

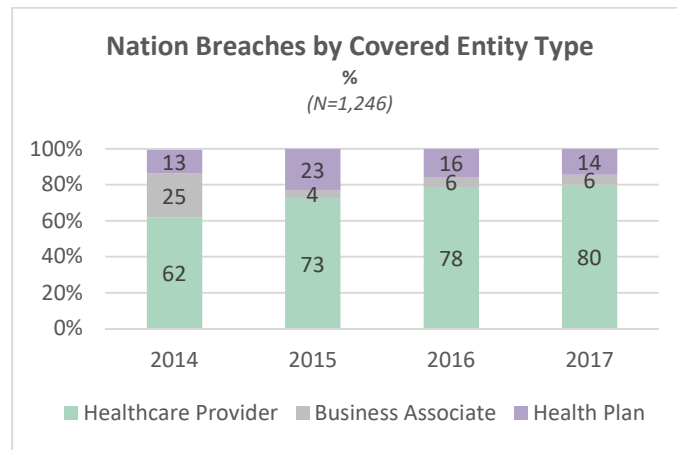
Appendix B

Top 10 Health Care Data Breaches 2017				
State	Organization	Records Compromised	Type of Breach	Covered Entity Type
KY	Commonwealth Health Corporation	697,800	Theft	Health Care Provider
MI	Airway Oxygen, Inc.	500,000	Hacking/IT Incident	Health Care Provider
PA	Women's Health Care Group of PA, LLC	300,000	Hacking/IT Incident	Health Care Provider
TX	Urology Austin, PLLC	279,663	Hacking/IT Incident	Health Care Provider
CA	Pacific Alliance Medical Center	266,123	Hacking/IT Incident	Health Care Provider
GA	Peachtree Neurological Clinic, P.C.	176,295	Hacking/IT Incident	Health Care Provider
AR	Arkansas Oral & Facial Surgery Center	128,000	Hacking/IT Incident	Health Care Provider
MI	McLaren Medical Group, Mid-Michigan Physicians Imaging Center	106,008	Hacking/IT Incident	Health Care Provider
PA	Harrisburg Gastroenterology LTD	93,323	Hacking/IT Incident	Health Care Provider
IN	VisionQuest Eyecare	85,995	Hacking/IT Incident	Health Care Provider

Appendix C



Appendix D



Appendix E



Top 10 States Ranking Records Compromised 2017			
Rank	State (State Population Ranking)	Records	Occurrences
1	KY (26)	768,648	10
2	MI (10)	677,235	14
3	TX (2)	573,216	33
4	CA (1)	449,834	34
5	PA (5)	411,997	11
6	GA (8)	301,136	11
7	IN (17)	176,272	9
8	AR (14)	154,000	2
9	FL (3)	146,090	23
10	NC (9)	142,447	9

For a listing of all states ranked by population size, visit:
simple.wikipedia.org/wiki/List_of_U.S._states_by_population.

Appendix F

All Maryland Breaches 2018			
Organization	Records Compromised	Type of Breach	Covered Entity Type
LifeBridge Health, Inc	538,127	Hacking/IT Incident	Healthcare Provider
Capital Digestive Care, Inc.	17,639	Unauthorized Access/Disclosure	Healthcare Provider
Special Agents Mutual Benefit Association	13,942	Unauthorized Access/Disclosure	Health Plan
CareFirst BlueCross BlueShield	6,200	Hacking/IT Incident	Health Plan
Westminster Ingleside King Farm Presbyterian Retirement Communities, Inc.	5,228	Hacking/IT Incident	Healthcare Provider
Serene Sedation, LLC	5,207	Hacking/IT Incident	Healthcare Provider
StatCare Group LLC	679	Hacking/IT Incident	Healthcare Provider

Appendix G



BREACH PORTAL REQUIRED INFORMATION

All information with an asterisk is required.

GENERAL Information Screen

Please supply the required general information for the breach.

* Report Type: What type of breach report are you filing?

- Initial Breach Report
- Addendum to Previous Report

If Addendum to Previous Report is selected:

* Do you have a valid breach tracking number? A breach tracking number would have been provided by OCR after January 1st, 2015. If you do not have a number please select 'No'.

- Yes
 - Breach Tracking Number: Please supply your breach tracking number.
- No

CONTACT Information Screen

Please supply the required contact information for the breach.

- Are you a Covered Entity who experienced a breach, and are filing on behalf of your organization?
- Are you a Business Associate who experienced a breach, and are filing on behalf of a Covered Entity?
- Are you a Covered Entity filing because your Business Associate experienced a breach?

If "Are you a Covered Entity who experienced a breach, and are filing on behalf of your organization" was selected:

FOR EXTERNAL USE: HHS OCR BREACH REPORT; REQUIRED INFORMATION

Covered Entity: Please provide the following information.

* Name of Covered Entity: (Name of Entity only (not of its representative), no abbreviations, no acronyms);

* Type of Covered Entity:

- Health Plan
- Healthcare Clearing House
- Healthcare Provider

* Street Address Line 1:

Street Address Line 2:

* City:

* State: -- Choose State --

* ZIP:

Covered Entity Point of Contact Information

* First Name:

* Last Name:

* Email:

* Phone Number: (Include area code):

Usage

- Home/Cell
- Work

If "Are you a Business Associate who experienced a breach, and are filing on behalf of a Covered Entity" was selected

Business Associate: Completion of this section is required if the breach occurred at or by a Business Associate or if you are filing on behalf of a Covered Entity.

2

FOR EXTERNAL USE: HHS OCR BREACH REPORT; REQUIRED INFORMATION

* Name of Business Associate: (Name of Business Associate only (not of its representative), no abbreviations, no acronyms):

* Street Address Line 1:

Street Address Line 2:

* City:

* State: -- Choose State --

* ZIP:

Business Associate Point of Contact Information

* First Name:

* Last Name:

* Email:

* Phone Number: (Include area code):

* Usage

- Home/Cell
- Work

Enter the contact information for all Covered Entities on whose behalf you are filing.

Covered Entity 1

* Name of Covered Entity: (Name of Entity only (not of its representative), no abbreviations, no acronyms):

* Street Address Line 1:

Street Address Line 2:

* City:

* State: -- Choose State --

* ZIP:

3

FOR EXTERNAL USE: HHS OCR BREACH REPORT; REQUIRED INFORMATION

Point of Contact Information

* First Name:

* Last Name:

* Email:

* Phone Number: (Include area code):

* Usage

- Home/Cell
- Work

* Type of Covered Entity:

- Health Plan
- Healthcare Clearing House
- Healthcare Provider

If "Are you a Covered Entity filing because your Business Associate experienced a breach" was selected:

Covered Entity: Please provide the following information.

* Name of Covered Entity: (Name of Entity only (not of its representative), no abbreviations, no acronyms):

* Type of Covered Entity:

- Health Plan
- Healthcare Clearing House
- Healthcare Provider

* Street Address Line 1:

Street Address Line 2:

* City:

* State: -- Choose State --

* ZIP:

4

Covered Entity Point of Contact Information

- * First Name:
- * Last Name:
- * Email:
- * Phone Number: (Include area code):

Usage

- Home/Cell
- Work

Business Associate: Completion of this section is required if the breach occurred at or by a Business Associate.

- * Name of Business Associate: (Name of Business Associate only, no abbreviations, no acronyms):
- * Street Address Line 1:
- Street Address Line 2:
- * City:
- * State: -- Choose State --
- * ZIP:

Business Associate Point of Contact Information

- * First Name:
- * Last Name:
- * Email:
- * Phone Number: (Include area code):

Phone Number

Usage

- Home/Cell
- Work

BREACH Information Screen

Breach Affecting: How many individuals are affected by the breach?

- 500 or More Individuals
- Fewer Than 500 Individuals

Breach Dates: Please provide the start and end date (if applicable) for the dates the breach occurred in.

- * Breach Start Date:
- * Breach End Date:

Discovery Dates: Please provide the start and end date (if applicable) for the dates the breach was discovered.

- * Discovery Start Date:
- * Discovery End Date:

* Approximate Number of Individuals Affected by the Breach:

* Type of Breach (drop-down instructions available in the portal):

- Hacking/IT Incident Help
- Improper Disposal Help
- Loss Help
- Theft Help
- Unauthorized Access/Disclosure Help

* Location of Breach:

- Desktop Computer
- Electronic Medical Record
- Email
- Laptop

FOR EXTERNAL USE: HHS OCR BREACH REPORT; REQUIRED INFORMATION

- Network Server
- Other Portable Electronic Device
- Paper/Films
- Other

* Type of Protected Health Information Involved in Breach:

- Clinical
 - Diagnosis/Conditions
 - Lab Results
 - Medications
 - Other Treatment Information
- Demographic
 - Address/ZIP
 - Date of Birth
 - Driver's License
 - Name
 - SSN
 - Other Identifier
- Financial
 - Claims Information
 - Credit Card/Bank Acct #
 - Other Financial Information
- Other

* Type of Protected Health Information Involved in Breach (Other):

[4,000 characters limit]

* Brief Description of the Breach:

[4,000 characters limit]

* Safeguards in Place Prior to Breach:

- None
- Privacy Rule Safeguards (Training, Policies and Procedures, etc.)
- Security Rule Administrative Safeguards (Risk Analysis, Risk Management, etc.)

7

FOR EXTERNAL USE: HHS OCR BREACH REPORT; REQUIRED INFORMATION

- Security Rule Physical Safeguards (Facility Access Controls, Workstation Security, etc.)
- Security Rule Technical Safeguards (Access Controls, Transmission Security, etc.)

NOTICE OF BREACH AND ACTIONS TAKEN Information Screen

Notice of Breach and Actions Taken: Please supply the required information about notices and actions.

* Individual Notice Provided Start Date:

* Individual Notice Provided Projected/Expected End Date:

Was Substitute Notice Required?

- Yes
 - Fewer than 10
 - 10 or more
- No

Was Media Notice Required?

- Yes
 - Select State(s) and/or Territories in which media notice was provided:
-- Choose State --
- No

* Actions Taken in Response to Breach:

- Adopted encryption technologies
- Changed password/strengthened password requirements
- Created a new/updated Security Rule Risk Management Plan
- Implemented new technical safeguards
- Implemented periodic technical and nontechnical evaluations
- Improved physical security
- Performed a new/updated Security Rule Risk Analysis
- Provided business associate with additional training on HIPAA requirements
- Provided individuals with free credit monitoring
- Revised business associate contracts
- Revised policies and procedures
- Sanctioned workforce members involved (including termination)

8

FOR EXTERNAL USE: HHS OCR BREACH REPORT; REQUIRED INFORMATION

- Took steps to mitigate harm
- Trained or retrained workforce members
- Other
 - o * Describe Other Actions Taken: [4,000 characters limit]

ATTESTATION Information Screen

Please complete the Attestation form.

Under the Freedom of Information Act (5 U.S.C. §552) and HHS regulations at 45 C.F.R. Part 5, OCR may be required to release information provided in your breach notification. For breaches affecting more than 500 individuals, some of the information provided on this form will be made publicly available by posting on the HHS web site pursuant to § 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5). Additionally, OCR will use this information, pursuant to § 13402(i) of the HITECH Act, to provide an annual report to Congress regarding the number and nature of breaches that are reported each year and the actions taken to respond to such breaches. OCR will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

I attest, to the best of my knowledge, that the above information is accurate.

* Name:

Date: [system generated]

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