Health Care Data Breaches:

A Changing Landscape

June 2017

Robert E. Moffit, PhD, Chair

Ben Steffen, Executive Director

Maryland Health Care Commission

This page intentionally left blank.

Table of Contents

This report was completed by Nikki Majewski, Chief, Health Information Technology, within the Center for Health Information Technology & Innovative Care Delivery under the direction of the Center Director, David Sharp, Ph.D. For information on this report, please contact Nikki Majewski at 410-764-3839 or by email at nicole.majewski@maryland.gov.

Introduction

Health care data breaches are likely to increase with expanded use of electronic health information. This can be attributed to security practices implemented by health care organizations that, while robust, are often less sophisticated when compared to other industries, such as the financial sector.[1] Large repositories containing medical records are valuable to cybercriminals as medical records include Social Security and credit card numbers, patient demographics, addresses, insurance identification numbers, and other medical information, and can sell on the black market for as much as 20 times the cost of a stolen credit card number.[2] Criminals use medical records to fraudulently bill insurance, receive free medical services, or obtain prescription medications.

An increasing surge of cyber-attacks[3] against health care organizations is contributing to more frequent data breaches. In 2016, the health care industry reported more breaches than any other year to date with cyber-attacks accounting for roughly 31 percent of all major health care breaches, an increase of 300 percent over three years.[4] Hacking incidents[5] in 2015 brought about some of the largest breaches in history involving health plans[6] and are considered to be a strong catalyst for health care to enhance security protections consistent with other business sectors.[7], [8] Industry experts see persistent cyber-attacks as the single greatest threat to the protection of health care data. This threat extends to critical health care operations and the physical welfare of patients.[9]

Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA or HIPAA Privacy Rule)[10] established national standards to ensure confidentiality of individuals' protected health information (PHI).[11] Individuals and organizations that meet the definition of a covered entity (i.e., health care providers, health plans, and health care clearinghouses) as well as business associates[12] must adhere to certain obligations under HIPAA.[13] The passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009 made enhancements to the HIPAA Privacy Rule.

[1] TechTarget, *FBI Notice: Healthcare Security Not as Mature as Other Verticals*, April 2014. Available at: searchsecurity.techtarget.com/news/2240219483/FBI-notice-Healthcare-security-not-as-mature-as-other-verticals.

[2] A medical record can sell for about $50 as compared to credit card information that sells for about $1.

[3] Cyber-attacks consist of deliberate attempts to gain unauthorized access to sensitive or proprietary information, usually through a computer system or network.

[4] In 2014, cyber-attacks were responsible for 10 percent of total major breaches; this increased to 21 percent in 2015.

[5] Hacking incidents can include, but are not limited to, phishing e-mails asking for sensitive information or attempts to gain unauthorized remote access to a network from a sophisticated threat actor determined to find a point of entry.

[6] Nation: Anthem BlueCross (80M records); Premera BlueCross (11M records); Excellus BlueCross BlueShield (10M records). Maryland: CareFirst BlueCross BlueShield (1.1M records).

[7] ISMG Network, *Anthem Breach Sounds a Healthcare Alarm*, February 2015. Available at: www.bankinfosecurity.com/anthem-follow-up-a-7878.

[8] See Appendix A for a listing of the top 10 health care breaches in 2015.

[9] TrapX Security, *Health Care Cyber Breach Research Report for 2016*, December 2016. Available at: deceive.trapx.com/rs/929-JEW-675/images/Research_Paper_TrapX_Health_Care.pdf?utm_source=PressRelease&utm_medium=2016_Year_End_Healthcare.

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

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

[12] An entity qualifies as a business associate if it creates, receives, maintains or transmits PHI on behalf of a covered entity or another business associate.

[13] A covered entity may engage with a business associate to perform certain health care activities and functions. For more information, visit: www.hhs.gov/hipaa/for-professionals/covered-entities/.

This includes a requirement that covered entities must provide notice of a breach to patients, the U.S. Department of Health & Human Services (HHS) Office for Civil Rights (OCR), and in certain circumstances, the media.[14, 15]

HITECH defines a breach as unauthorized acquisition, use, or disclosure of PHI which compromises the security or privacy of PHI. Impermissible use or disclosure includes PHI that is stolen or improperly accessed, sent inadvertently to the wrong provider, or viewed by an unauthorized individual.[16] Information on breaches affecting 500 or more individuals is searchable through an online portal maintained by OCR. The portal includes details on breaches that OCR has investigated, including name of covered entity, state, covered entity type, number of individuals affected, breach submission date, type of breach, and location of breached information.[17]

About this Report

The Maryland Health Care Commission (MHCC) analyzed data from the OCR breach portal from 2010 through 2016 to assess reported breaches in Maryland. Data used in the assessment only includes breaches reported during this time period that OCR has investigated and closed (i.e., 32 in Maryland and 1,780 nationally). This information is intended to inform stakeholders about the increasing prevalence of health care breaches, and includes recommendations on how to enhance security processes to prepare for and mitigate the effects of new and evolving cyber threats. Findings will be used by MHCC to inform security education and awareness initiatives. Recommendations for safeguarding electronic PHI and breach remediation align with industry best practices; the information included is not an exhaustive list and other measures for mitigating risk should be considered.

Breaches by Covered Entity Type

Since 2010, health care providers (providers), as compared to other covered entities, have experienced more than half of all breaches, with the nation exceeding Maryland by about 10 percent (Figure 1).[18] Maryland has experienced more fluctuation in breaches among covered entities within the past several years. The need for providers to take a more proactive and comprehensive approach to protecting their information assets stands out in 2016 as provider organizations accounted for all breaches in Maryland and about 78 percent nationally (Figures 2 and 3). In general, varying degrees of privacy and security readiness among providers can present challenges for mitigating risks. This includes a lack of controls to safeguard PHI, outdated policies and procedures or non-adherence to existing ones, and inadequate end-user training, among other things.[19] Increased risk of a breach can also be attributed to how providers have pieced together their health information technology (health IT) infrastructure over time, potentially increasing exposure to vulnerabilities that may not be as

[14] HIPAA requires a business associate to notify the covered entity of a potential breach within 60 days of discovery.

[15] Breach notification requirements vary based on whether a breach affects 500 or more individuals or fewer than 500 individuals. For more information, visit: www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/.

[16] An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate demonstrates there was a low probability that PHI was compromised based on a risk assessment. For more information, visit: www.hhs.gov/hipaa/for-professionals/breach-notification/.

[17] For more information on the OCR breach portal, visit: ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[18] Reporting of breaches is done by the covered entity, so it is possible that some breaches are incorrectly attributed to a health care provider despite originating from a business associate.

[19] Healthcare IT News, *Healthcare Organizations at Risk for more Breaches*, March 2011. Available at: www.healthcareitnews.com/news/healthcare-organizations-risk-more-breaches.

easy to detect.[20] Ambulatory practices, hospitals, and outpatient facilities are the most common provider types required by OCR to implement corrective actions to achieve HIPAA compliance.[21]

As providers become more reliant on business associates, they are accepting not only essential assistance but increased cybersecurity risk. In general, the way breaches are reported by covered entities often does not indicate a business associate was responsible.[22, 23] Business associates perform many functions involving use and disclosure of PHI on behalf of a covered entity. While reported breaches among business associates overall trails providers by about one-third (Figure 1), small and midsized business associates are often more vulnerable due to their lower budgets for privacy and security and less formal monitoring and auditing programs.[24] According to a study conducted by the Ponemon Institute, only about half of business associates report their policies and procedures, personnel, technology, and resources are adequate to prevent or quickly detect incidents of unauthorized access, loss, or theft of patient data. In addition, roughly half believe their incident response process is adequate.[25]

In recent years, cyber-attacks contributed to an uptick in breaches reported by health plans, particularly in Maryland in 2014 and 2015 (Figures 2 and 3). The largest of these breaches experienced by CareFirst Blue Cross BlueShield in 2015 exposed nearly 1.1 million records of current and former health insurance customers. During this same time period, health plans nationally experienced record data breaches (Figure 3). Anthem reported the largest data breach in health care history that compromised nearly 80 million records.[26] The Anthem breach in particular raised awareness about health care organizations ability to protect electronic data. Health plans often have legacy systems attached to new systems making them less synchronized and more susceptible to vulnerabilities.

[20] Farrow–Gillespie & Health, *Healthcare Providers' Risk of Data Breach*, March 2017. Available at: www.fghlaw.com/hipaa-data-breach/.

[21] US. Department of Health & Human Services, *Enforcement Highlights*, as of February 28, 2017. Available at: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

[22] The OCR reporting portal includes an option labeled, "Are you a covered entity filing on behalf of a business associate?" Some covered entities do not think they are filing on a business associate's behalf, so they don't select that option.

[23] Healthcare Informatics, Study: *30 Percent of Patient Data Breaches Involve Business Associates*, September 2016. Available at: www.healthcare-informatics.com/news-item/cybersecurity/study-30-percent-patient-data-breaches-involve-business-associates.

[24] Grant Thornton, *Monitor Business Associates to Help Prevent Breaches*, August 2016. Available at: www.grantthornton.com/library/articles/health-care/2016/Business-associates-breaches-webcast-follow-up.aspx.

[25] Ponemon Institute, *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data*, May 2016.

[26] See Appendix A for a listing of the top 10 health care breaches in 2015.

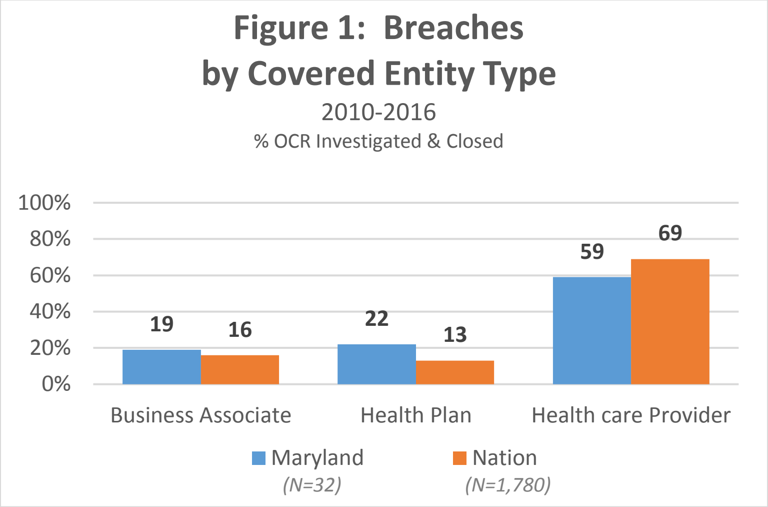


Figure 1: Breaches by Covered Entity Type

2010-2016

% OCR Investigated & Closed

Note: Health care clearinghouses and unknown entity type accounts for less than 2 percent of all national breaches.

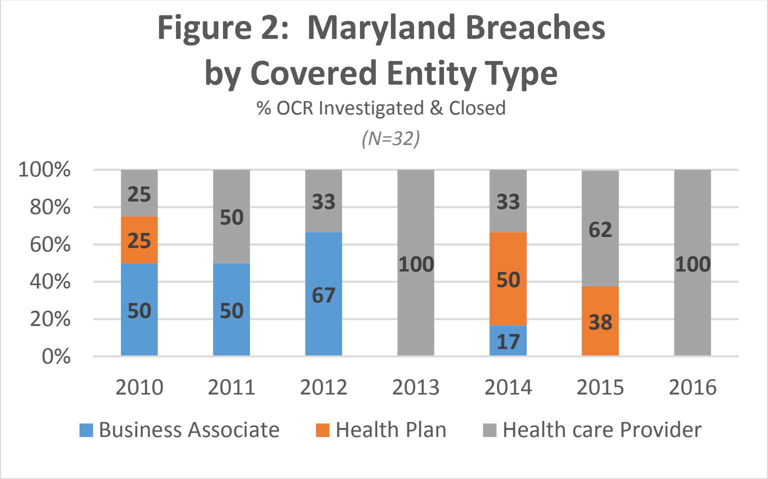


Figure 2: Maryland Breaches by Covered Entity Type

% OCR Investigated & Closed

(N=32)

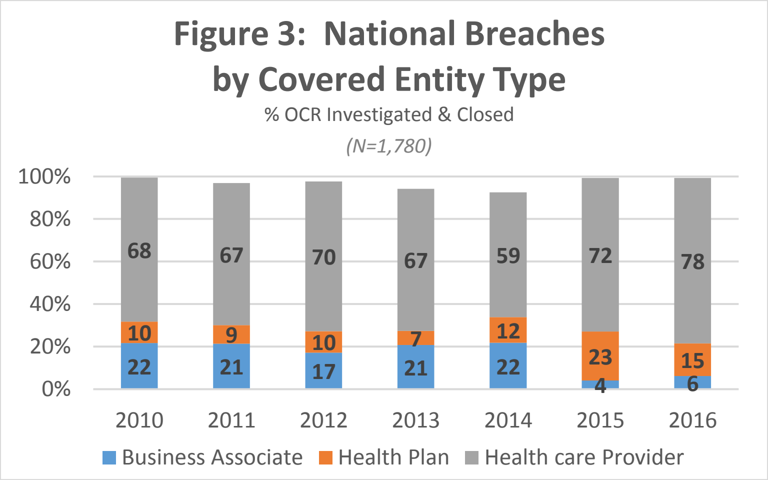


Figure 3: National Breaches by Covered Entity Type

% OCR Investigated & Closed

(N=1,780)

Note: Covered entity type is unknown for a small portion breaches (2010 – 1%; 2011 – 3%; 2012 – 2%; 2013 – 5%; 2014 – 7%; 2015 – 1%; 2016 – 1%). Healthcare clearinghouses accounted for 1% of breaches in 2011 and 2013. These percentages are not illustrated in the chart above.

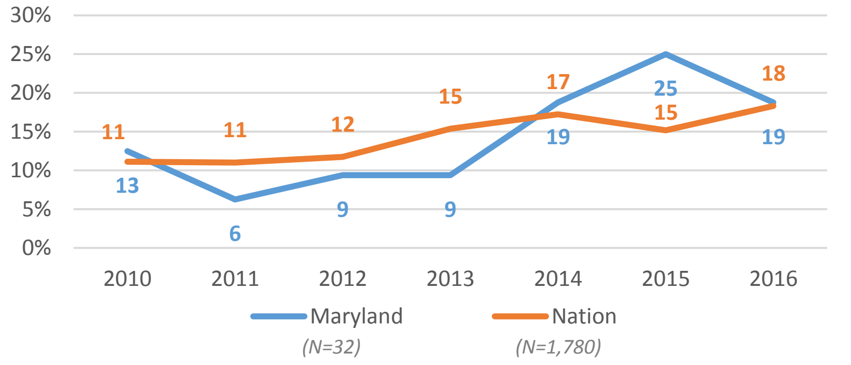
Frequency and Impact

From 2011 through 2013, breaches in Maryland trailed the nation by about 4.7 percent. Since then, Maryland breaches have exceeded the nation with a disconcerting number of occurrences in 2015 (Figure 4). Overall, 2015 stands out for both Maryland and the nation given the number of individual health care records that were exposed or stolen, with breaches collectively affecting over 114 million individuals.[27] The largest single breach involving Anthem represents over 70 percent of all records compromised. In comparison, an estimated 41 million health care records were compromised between 2010 through 2014.

Frequency and impact of breaches continues to amplify as the health care industry embraces a digital future through increased adoption of electronic health records as well as cloud-based services to support various Internet-based health care platforms.[28] Information security at health care organizations face significant challenges with the growing number of devices, users, and applications that are connected to networks. These challenges, which include bring your own device (BYOD)[29] and the Internet of Things (IoT)[30], are creating new vulnerabilities for health care organizations.[31] Some breaches go unreported, and breaches involving fewer than 500 individuals are not required to be publicly reported on the OCR portal.

Figure 4: Occurance of Breaches by Year

% OCR Investigated & Closed



Common Types of Breaches

In addition to changes in frequency and impact of breaches within the last seven years, there has also been a shift in the way PHI has been breached. The top three types of breaches include: hacking/IT incident, theft, and unauthorized access/disclosure (Figure 5). Breaches involving a hacking/IT incident and unauthorized access/disclosure have steadily increased since 2010, growing at a rate of over 50 percent. Within the past three years, the trend in hacking/IT incidents increased most significantly with a growth rate of 92 percent and was the leading cause of breaches in 2016 (Figure

[27] See Appendix A for information on the top 10 health care breaches in 2015.

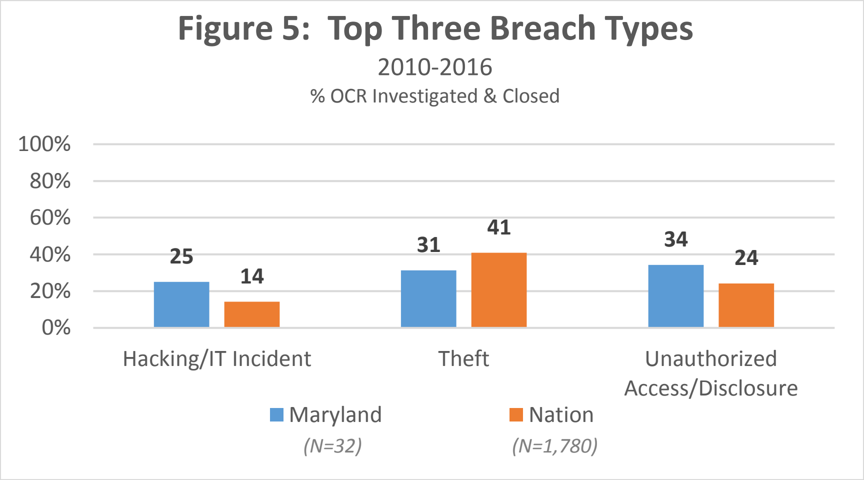
[28] Liu, Vincent, Mark A. Musen, and Timothy Chou. "Data Breaches of Protected Health Information in the United States." JAMA 313.14 (2015): 1471–1473. PMC. Web. 10 Mar. 2017.

[29] BYOD is the practice of allowing employees to use their own computers, smartphones, and other electronic devices for work purposes.

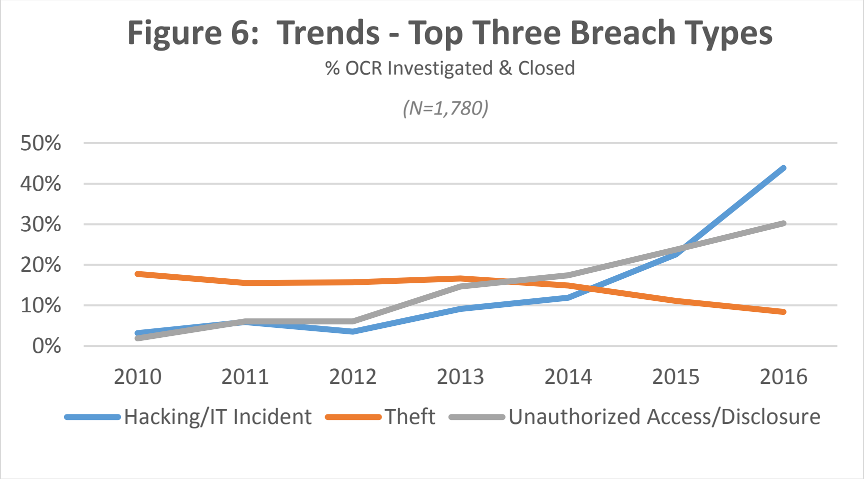
[30] IoT is a concept of connecting electronic devices that capture and monitor data to the Internet and each other.

[31] HealthIT Security, *Why Cybersecurity Breaches Are on the Rise for Healthcare*, November 2014. Available at: healthitsecurity.com/news/cybersecurity-breaches-rise-healthcare/.

6/Table 1).[32] The rate of breaches involving theft is decreasing (Figure 6/Table 1). Researchers remain divided about the main causes of breaches despite having knowledge about the common types. Some attribute increases to widespread use of health IT; human error is thought to be another leading cause.[33] Internal issues such as employee negligence, third-party malfunctions, and stolen computing devices continue to put patient data at risk.[34]



Note: Other types of breaches occur involving a combination of the above.



[32] See Appendix B for information on growth rate.
[33] Perspectives in Health Information Management, *What Caused the Breach? An Examination of Use of Information Technology and Health Data Breaches*, 2014. Available at: perspectives.ahima.org/what-caused-the-breach-an-examination-of-use-of-information-technology-and-health-data-breaches/#.
[34] Ibid 25.

Table 1: Growth - Top Three Breach Types
%

Type of Breach	2010	2011	2012	2013	2014	2015	2016	Growth Rate 2010-2016	Growth Rate 2014-2016
Hacking/IT Incident	3	6	4	9	12	23	44	55	92
Theft	18	16	16	17	15	11	8	-12	-24
Unauthorized Access/ Disclosure	2	6	6	15	17	24	30	59	32

Note: Information above represents compound annual growth rate.

Assessing the Impact

The residual effects of a breach can include financial and reputational harm. This can be attributed to the loss of sensitive and propriety information, disruption to regular operations, and the impact on consumer trust, confidence, and loyalty.[35] Following a breach, health care organizations can incur expenses from hardware and software upgrades required to address security gaps. Other costs include fees for providing breach victims with credit and identity monitoring services and regulatory fines.[36] Reputational damage can have a downstream effect on patient trust about a health care organization's ability to safeguard their electronic health information. A study conducted by TransUnion Healthcare, a global risk information provider, found that nearly 7 in 10 patients would avoid providers that experience a breach.[37, 38] Historically, a primary concern has been about reputational impact following public disclosure. However, research suggests the effects on reputation can be even greater when the underlying cause of a breach could have been prevented and/or the health care organization is viewed as not responding well.[39]

In Maryland, two high profile hacking incidents emphasize the importance of organizational preparedness and response to a breach or potential breach. While discovery of a breach after only a year of its genesis is fairly standard, initiating response and recovery efforts in the hours and days that follow is crucial to securing information systems. The full scope of the CareFirst breach in 2015 was discovered about 10 months after intrusion to their systems took place.[40] This breach compromised member information used to access CareFirst online services, such as usernames, birthdates and subscriber identification numbers. While it was determined that password information was encrypted and stored in a separate system as a safeguard against such attacks, CareFirst exercised caution by blocking member access to impacted accounts until a new password

[35] Experian, *The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches*, April 2010. Available at: www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[36] Refer to the section entitled, *Regulatory Considerations,* for information on regulatory fines.

[37] Responses varied among consumer groups. While 73 percent of younger respondents ages 18 to 34 said they were likely to switch health care providers, about 64 percent of respondents older than 55 indicated they were not likely to consider switching health care providers following a breach.

[38] TransUnion, *Nearly Seven in 10 Patients Would Avoid Healthcare Providers That Experience a Data Breach*, March 2015. Available at: newsroom.transunion.com/transunion-survey-nearly-seven-in-10-patients-would-avoid-healthcare-providersthat-undergo-a-data.

[39] BakerHostetler, *Is Your Organization Compromise Ready?*, 2016. Available at: www.bakerlaw.com/files/uploads/Documents/Privacy/2016-Data-Security-Incident-Response-Report.pdf.

[40] In April 2015, CareFirst determined an intrusion of its systems occurred sometime in June 2014. CareFirst subsequently offered affected customers two years of free credit monitoring services.

and username was created.[41] A non-breach incident experienced by MedStar in 2016 involved unidentified hackers encrypting data, bringing the systems of one of Maryland's largest health care systems to a halt. MedStar's decision to take down all system interfaces until the incident was resolved left hospital staff relying on older techniques, such as paper records and fax machines.[42]

Minimizing Risk through Preparedness and Response

Hacking related incidents have, in part, prompted a new sense of urgency in Maryland to ensure health care organizations have adequate strategies in place for responding to security incidents. An environmental scan of hospital cybersecurity conducted by MHCC in the spring of 2016 found that over one-half of hospitals report modifying their incident response plans to include more specific cybersecurity procedures. About a third of hospitals test their incident response plans, which can include mock exercises to practice and assess hospital capabilities for responding to a cyber incident.[43] Incident response plans should be robust, including not only breach response protocols but rapid response protocols to avoid a breach. Key elements of incident response plans are people, processes, and technology extending beyond the IT department and include executive management, human resources, marketing, legal, and vendors with access to data, among others.[44]

Another important aspect of minimizing risk is understanding the issue of human error as networks are built, operated, and maintained by people. Some experts tend to debate the effectiveness of security training; yet, human error has been identified as a significant contributor to security incidents and HIPAA penalties are a solid indicator that lack of awareness and training is no excuse for a breach. While phishing, hacking, and malware were the leading causes of security incidents in 2016, the underlying causes were often attributed to human error. The human element is a driving force for health care organizations to develop robust security education and awareness programs. In Maryland, all health systems and about three quarters of community-based hospitals provide cybersecurity training to employees.[45]

Establishing a security-minded culture helps reduce the risk of a breach. In general, security training should include all employees and business associates with system access. Training basics encompass things such as how to identify and avoid phishing attempts[46] and other forms of social engineering[47], and what to do when employees think they may have been targeted. Additionally, training should be targeted to specific groups, highlighting specific areas of responsibility, and involve competency testing. Initial training is an important part of a new employee onboarding process, but frequency of

[41] Security Week, *CareFirst Data Breach Impacts 1.1 Million*, May 2015. Available at: www.securityweek.com/carefirst-data-breach-impacts-11-million.

[42] Baltimore Sun, *MedStar Hack Shows Risks that Come with Electronic Health Records*, April 2016. Available at: www.baltimoresun.com/health/bs-md-medstar-healthcare-hack-20160402-story.html.

[43] MHCC, *Hospital Cybersecurity: Evolving Threats Require New Approaches*, October 2016. Available at: mhcc.maryland.gov/mhcc/pages/hit/hit/documents/HIT_Cybersecurity_Assessment_Brf_20161025.pdf.

[44] Grant Thornton, *Prevention and triage apply in hospital cybersecurity*, 2015. Available at: https://www.grantthornton.com/~/media/content-page-files/health-care/pdfs/2015/Prevention-and-triage-in-hospital-cybersecurity.ashx.

[45] Ibid 43.

[46] An attempt to obtain sensitive information such as usernames and passwords for malicious reasons by disguising as a trustworthy entity in an electronic communication.

[47] A technique, such as a phishing attempt, used to manipulate individuals into divulging confidential or personal information in order to gain system access. It does not exploit vulnerabilities in the system itself but instead attempts to exploit vulnerabilities in humans using the system. For more information on different types of social engineering attacks, visit: www.smartfile.com/blog/social-engineering-attacks/.

training plays a major role in ensuring good security hygiene. Experts recommend quarterly training, as well as training following a security incident.[48, 49]

Regulatory Considerations

HHS enforces HIPAA and HITECH mandates through compliance investigations and audits performed by OCR.[50] Fines for non-compliance are based on the level of negligence and can range from $100 to $50,000 per violation (or record).[51] Following a breach, health care organizations should not underestimate the importance of their remediation efforts. Oftentimes, organizations focus largely on notification requirements as part of their incident response; however, it's also critical to prepare for responding to an OCR investigation by undertaking corrective actions that may help resolve an investigation quickly. The following best practices not only help during an investigation, but also provide basic protections to prevent breaches:[52]

- Documentation of the incident response, investigation, mitigation, notification of individuals, substitute notice, and media notice provided;
- Established policies and procedures governing privacy and security;
- Evidence of education and awareness training programs, including attendance logs;
- Implemented sanctions policy and evidence of any disciplinary action taken;
- Security risk analysis conducted by the organization over a several-year period preceding the incident;
- Risk mitigation plans developed as a result of risk analyses;
- Vendor/business associate agreements in place, regardless of whether a vendor caused the incident, and including internal business associate agreements with corporate entities; and
- Evidence of corrective action taken.[53]

While health care breaches involving 500 or more individuals have routinely been subject to investigation by OCR, there is a shifting focus to actively investigate breaches of PHI affecting fewer than 500 individuals. In August 2016, OCR announced plans to more broadly investigate smaller breaches of PHI. The intent is to evaluate the primary and likely causes of security incidents, and develop appropriate corrective actions to ensure a comprehensive approach to risk management that includes implementing physical, technical, and administrative safeguards to secure PHI. Covered entities and business associates can anticipate an increase in the volume of enforcement actions by OCR for small-scale PHI breaches.[54]

[48] OnRamp, *HIPAA Security and Awareness Training: An Integral Part of the Compliance Strategy*, July 2016. Available at: www.onr.com/blog/hipaa-security-awareness-training-integral-part-compliance-strategy/.

[49] See Appendix C for additional information on resources to minimize risks.

[50] In conjunction with OCR, state attorneys general may respond to health care breaches in the form of civil investigative demands or by issuing their own separate consent orders. In addition, health plans often must answer to additional regulatory bodies, such as state departments of insurance and the National Association of Insurance Commissioners.

[51] Violations can also carry criminal charges that could result in jail time.

[52] BakerHostetler, *Deeper Dive: The Changing Landscape of Healthcare Data Breaches*, April 2016. Available at: www.dataprivacymonitor.com/hipaahitech/deeper-dive-the-changing-landscape-of-healthcare-data-breaches/.

[53] Ibid 39.

[54] Ropes & Gray, *OCR Announces Initiative to Amplify Investigations of Breaches Affecting Fewer than 500 Individuals*, September 2016. Available at: www.ropesgray.com/newsroom/alerts/2016/September/OCR-Announces-Initiative-to-Amplify-Investigations-of-Breaches-Affecting-Fewer-than-500-Individuals.aspx.

Historically, the health care industry has focused almost exclusively on the protection of patient records and less on minimizing threats to electronic health information.[55] Security incidents involving a non-breach of PHI pose significant threats to patient health. This is evident from the rise in ransomware where hackers deny access to data. The impact on health care operations can be substantial, forcing them to redirect care delivery techniques until systems are able to be brought back online. Federal and Maryland laws describe a breach as when information is inappropriately accessed or released; however, the laws lack clarity regarding notification requirements to the public when data is locked by hackers but not stolen.[56]

Risk Management through Third Party Reviews

Health care organizations are under increasing pressure to minimize security risks by demonstrating that processes and controls are in place to detect, respond to, and mitigate the effects of a breach or cyber-attack. IT risk management strategies must be comprehensive and dynamic to prevent or alleviate the potential consequences of a security incident. Incorporating independent reviews as part of a comprehensive strategy provides additional assurances to health care organizations in reducing risk. While many entities report an increase in IT security spending to better address security concerns, approximately 80 percent of breaches are discovered by independent third party reviews. Remarkably, internal discovery of threats stands at a mere 10 percent and has been on a downward trend within the past decade.[57]

Third party reviews offer a beneficial level of independent examination of risk management plans and procedures and can enable corrective actions to be deployed more quickly. Insurance underwriters of cybersecurity policies are beginning to recognize these benefits and are increasingly looking for independent third party validation as a prerequisite before issuing coverage.[58] The American Institute of Certified Public Accountants (AICPA) developed a risk management framework to examine non-financial reporting controls as they relate to five trust service principles: security, availability, processing integrity, confidentiality, and privacy.[59] Findings are detailed in a Service Organization Control (SOC) 2 report, which is intended to meet the needs of a broad range of users that need assurance about the adequacy of controls at a service organization.[60, 61] Some level of risk will always be inherent, particularly as health care increases its reliance on cloud-based technology. Sustainability of a health care organization is contingent upon their ability to align risk management with strategic planning.

[55] Independent Security Evaluators, *Securing Hospitals – A Research Study and Blueprint*, February 2016. Available at: www.securityevaluators.com/hospitalhack/securing_hospitals.pdf.

[56] Ibid 42.

[57] The American Journal of Accountable Care, *Make Accreditation Part of Your IT Risk Management Strategy*, January 2017. Available at: www.ajmc.com/contributor/lee-barrett/2017/01/Make-accreditation-part-of-your-IT-risk-management-strategy.

[58] Ibid 57.

[59] For more information on AICPA trust service principles visit: www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/TrustDataIntegrityTaskForce.aspx.

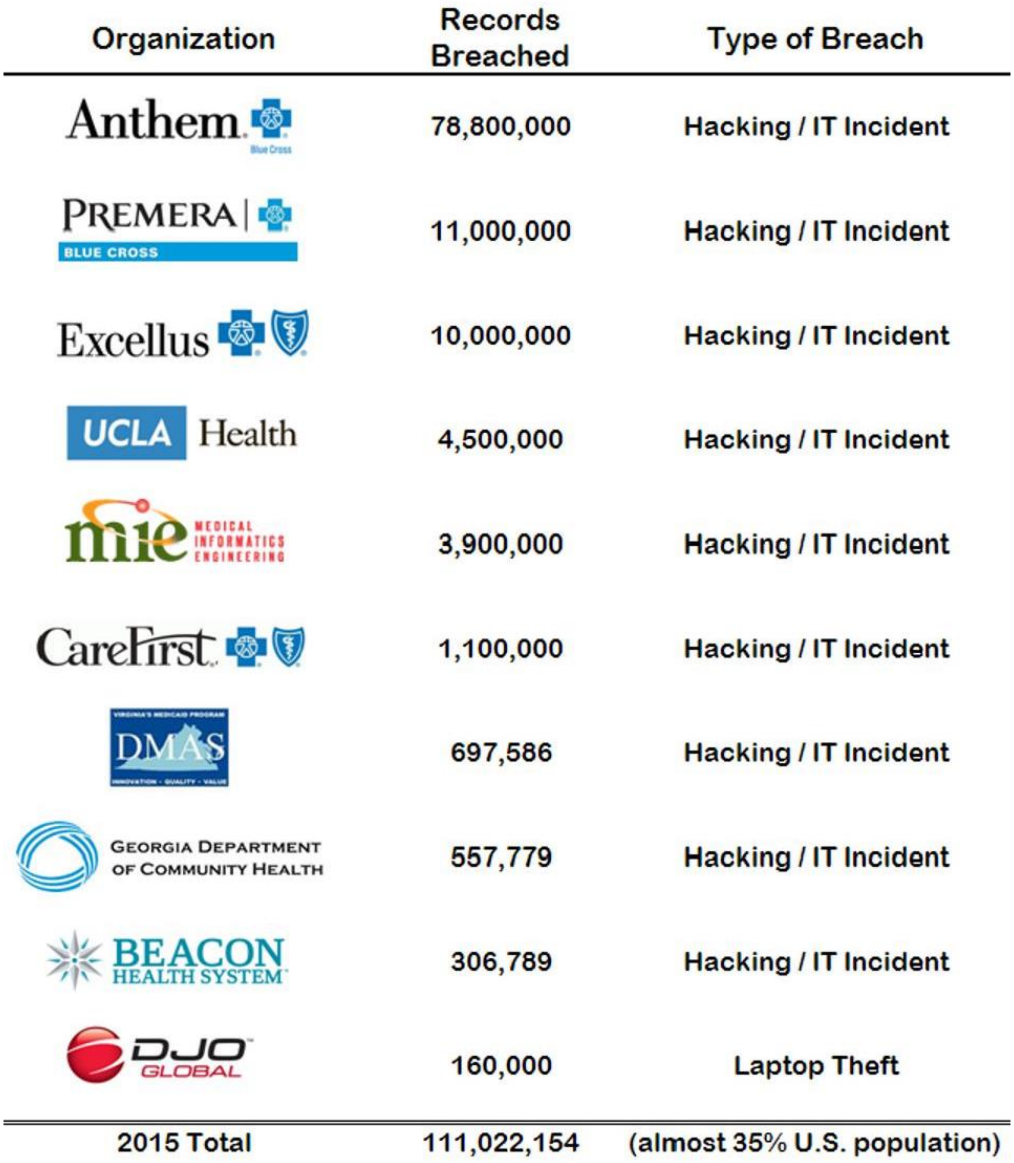
[60] A review does not require evaluation of all trust service principles and can be limited to only those principles that are relevant to the services being performed.

[61] SOC 2 reports come in two forms: Type I reports on policies and procedures placed in operation at a specific moment in time; Type II reports on policies and procedures over a period of at least six months and are considered more comprehensive and reliable than Type I. For more information, visit: www.netgainit.com/soc.

Remarks

More work is needed in Maryland to guard against increased risks that health care organizations face in protecting PHI. The impact of a breach or cyber-attack can have multilayered consequences. In addition to regulatory fines and other costs to implement corrective actions, the impact can be damaging on individuals and the reputation of a health care organization. Many breaches and cyber-attacks are not detected for an extended period of time, which allows hackers unfettered system access to PHI. Adopting strategies aimed at preventing IT system intrusion and detecting these inevitable events is crucial. Equally important are the comprehensive security testing programs that ensure controls are in place to guard against emerging threats.

Appendix A: Top 10 Health Care Data Breaches 2015



Organization	Records Breached	Type of Breach
Anthem Blue Cross	78,800,000	Hacking / IT Incident
PREMERA | BLUE CROSS	11,000,000	Hacking / IT Incident
Excellus	10,000,000	Hacking / IT Incident
UCLA Health	4,500,000	Hacking / IT Incident
mie MEDICAL INFORMATICS ENGINEERING	3,900,000	Hacking / IT Incident
CareFirst	1,100,000	Hacking / IT Incident
VIRGINIA'S MEDICAID PROGRAM DMAS INNOVATION · QUALITY · VALUE	697,586	Hacking / IT Incident
GEORGIA DEPARTMENT OF COMMUNITY HEALTH	557,779	Hacking / IT Incident
BEACON HEALTH SYSTEM	306,789	Hacking / IT Incident
DJO GLOBAL	160,000	Laptop Theft
2015 Total	111,022,154	(almost 35% U.S. population)

Source: Forbes, *Data Breaches In Healthcare Totaled Over 112 Million Records in 2015*, December 2015. Available at: www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#357472057b07.

Appendix B: Breaches by Type

The table below details baseline information on the number of breaches for each type of breach specified. These figures were used to calculate the compound annual growth rate (CAGR) between 2010 -2016 and 2014-2016. CAGR is the measure of growth over multiple periods and illustrates the average rate of growth for each type of breach.

Growth - Top Three Breach Types

Type of Breach	2010	2011	2012	2013	2014	2015	2016	Growth Rate 2010-2016	Growth Rate 2014-2016
	(#)							(%)	
Hacking/IT Incident	8	15	9	23	30	57	111	*55*	*92*
Theft	129	113	114	121	108	81	61	*-12*	*-24*
Unauthorized Access/ Disclosure	8	26	26	63	75	102	130	*59*	*32*

Note: Information above was used to calculate compound annual growth rate.

Appendix C: Risk Management Resources

Essential to minimizing risk is enhancing organizational readiness. The following resources provide information on best practices for enhancing IT risk management.

A BakerHostetler data security incident response report recommends a "compromise ready" approach to risk management. This approach is designed to assist health care organizations in implementing the right capabilities to prevent, detect, and respond to a security incident. (Figure 7).[62] Generally, once an attacker gains access to a network, they then take time to learn about a network and try to escalate privileges.[63] BakerHostetler recommends the following three areas where organizations can improve the most:

- Detect incidents sooner;
- Contain them faster after detection; and
- Maintain good logs to facilitate more precise determination of what occurred before an attack was stopped.[64]

Figure 7: Key Components of Being Compromise Ready

1. Preventative and detective security capabilities
2. Threat information gathering
3. Personnel awareness and training
4. Proactive security assessments that focus on identifying the location of critical assets and data and implementing reasonable safeguards and detection capabilities around them
5. Assessing and overseeing vendors
6. Developing, updating, and practicing incident response plans
7. Understanding current and emerging regulatory hot buttons
8. Evaluating cyber liability insurance.

Source: BakerHostetler

Experian, an industry leader in data breach resolution, offers a *Data Breach Response Guide* intended to support IT and other health care executives in putting together an enterprise-wide plan to prepare for and respond to a breach. The guides includes strategies for improving security posture, including communicating with the C-suite, creating a plan, practicing the plan, responding to a breach, auditing the plan, and finding helpful resources. The guide also includes a readiness assessment, consisting of questions that evaluate the effectiveness of plans in place for responding to a breach.[65]

The MHCC in collaboration with stakeholders[66] developed a Cybersecurity Self-Assessment Tool to support small health care organizations in assessing cybersecurity readiness. The tool uses select elements from the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The NIST CSF is recognized as a set of optional standards, best practices, and recommendations for improving cybersecurity at the organizational level.[67] The tool consists of a

[62] Ibid 39.

[63] Escalation of privileges is an attack that involves intrusion to a network that seeks to take advantage of programming errors or design flaws to enable an attacker access to the network and its associated data and applications.

[64] Ibid 39.

[65] For more information, visit: www.experian.com/data-breach/2015-2016-response-guide.html?ecs_dbres_Q4_Newsletter_2015_16_response_guide.

[66] Includes the Maryland Hospital Association; MedChi, The Maryland State Medical Society; LifeSpan Network; and Health Facilities Association of Maryland.

[67] The NIST CSF was developed through a collaborative process with experts in the federal government and private sector. For more information, visit: www.nist.gov/cyberframework.

series of evaluation statements intended to help health care organizations identify potential gaps in cybersecurity readiness.[68] The statements are grouped into people, processes, policies, and technology and contains industry best practices endorsed by the NIST CSF. A copy of the tool is available here:

mhcc.maryland.gov/mhcc/pages/hit/hit/documents/Cybersecurity_Self-Assessment_Tool.pdf.

[68] Results from the tool are intended to help inform health care organizations about the adequacy of existing cyber protections and do not constitute legal advice.

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