Health Care Data Breaches: 2017 Findings

September 2018

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

Maryland Health Care Commission
# 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 records\(^1\) 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 more than other breach types\(^2\) 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 updates\(^8\), weak passwords, and uncredentialed access\(^9\) 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.

---

\(^1\) 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.


\(^5\) 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/

\(^6\) Wired, Equifax officially has no excuse, September 2017. Available at: wired.com/story/equifax-breach-no-excuse/.


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 authentication\textsuperscript{14}, preventing unauthorized software installations, and removing or blocking unnecessary software and browser plugins (e.g., installing antivirus software and ad-blocking).\textsuperscript{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.\textsuperscript{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)\textsuperscript{17} and business associates (BA)\textsuperscript{18} in 2017 to the Department of Health & Human Services, Office for Civil Rights (OCR). Data was retrieved from the OCR online portal.\textsuperscript{19} This information brief presents a summary of findings from breaches reported in Maryland and the nation and an update on key trends.\textsuperscript{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).\textsuperscript{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.\textsuperscript{24}

\textsuperscript{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).


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

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

\textsuperscript{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.


\textsuperscript{21} See Appendix A for list of Maryland Breaches.

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

\textsuperscript{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.

\textsuperscript{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. 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.

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Maryland</td>
<td>6</td>
<td>273,719</td>
<td>8</td>
<td>1,131,380</td>
<td>6</td>
<td>669,919</td>
<td>8</td>
<td>55,961</td>
<td>28</td>
<td>2,130,979</td>
</tr>
<tr>
<td>Nation</td>
<td>294</td>
<td>12,285,589</td>
<td>269</td>
<td>113,265,216</td>
<td>326</td>
<td>16,626,349</td>
<td>359</td>
<td>5,138,179</td>
<td>1,248</td>
<td>147,315,333</td>
</tr>
</tbody>
</table>

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. 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). 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. 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. 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.

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.
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.
31 Healthcare IT 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.
Breath 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, 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. 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.

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.
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, 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).
\(^{38}\) 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>
<thead>
<tr>
<th>Comparative Ranking</th>
<th>State [Breach Occurrences]</th>
<th>Records Compromised</th>
<th>Overall Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IN (9)</td>
<td>176,272</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>MO (12)</td>
<td>140,389</td>
<td>11</td>
</tr>
<tr>
<td>3</td>
<td>CO (12)</td>
<td>65,982</td>
<td>17</td>
</tr>
<tr>
<td>4</td>
<td>MD (8)</td>
<td>55,961</td>
<td>20</td>
</tr>
<tr>
<td>5</td>
<td>NJ (8)</td>
<td>46,098</td>
<td>21</td>
</tr>
<tr>
<td>6</td>
<td>AZ (8)</td>
<td>35,339</td>
<td>24</td>
</tr>
<tr>
<td>7</td>
<td>CT (7)</td>
<td>27,844</td>
<td>28</td>
</tr>
</tbody>
</table>

**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) 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>
<thead>
<tr>
<th>Breach Location(s) Cited</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Occurrences</td>
<td>Records</td>
</tr>
<tr>
<td></td>
<td>N=6</td>
<td>N=669,919</td>
</tr>
<tr>
<td>Desktop Computer</td>
<td>17</td>
<td>1</td>
</tr>
<tr>
<td>Desktop Computer/ EMR</td>
<td>17</td>
<td>&lt;1</td>
</tr>
<tr>
<td>EMR</td>
<td>17</td>
<td>&lt;1</td>
</tr>
<tr>
<td>EMR/ Network Server</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>e-Mail</td>
<td>17</td>
<td>&lt;1</td>
</tr>
<tr>
<td>Network Server</td>
<td>17</td>
<td>97</td>
</tr>
<tr>
<td>Other Portable Electronic Device</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other</td>
<td>17</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Breach Location Cited</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Occurrences</td>
<td>Records</td>
</tr>
<tr>
<td></td>
<td>N=326</td>
<td>N=16,640,090</td>
</tr>
<tr>
<td>Desktop Computer</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>e-Mail</td>
<td>15</td>
<td>6</td>
</tr>
<tr>
<td>EMR</td>
<td>11</td>
<td>3</td>
</tr>
<tr>
<td>Laptop</td>
<td>9</td>
<td>5</td>
</tr>
<tr>
<td>Network Server</td>
<td>30</td>
<td>80</td>
</tr>
<tr>
<td>Paper/Films</td>
<td>24</td>
<td>6</td>
</tr>
<tr>
<td>Other Portable Electronic Device</td>
<td>6</td>
<td>&lt;1</td>
</tr>
<tr>
<td>Other</td>
<td>10</td>
<td>32</td>
</tr>
</tbody>
</table>

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 2018 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.

<table>
<thead>
<tr>
<th>Table 5. Maryland and Nation Breaches</th>
<th>As of August 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Reported Breaches</td>
</tr>
<tr>
<td>Maryland</td>
<td>7</td>
</tr>
<tr>
<td>Nation</td>
<td>221</td>
</tr>
</tbody>
</table>

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). A hacking/IT breach at a Baltimore health system that lead to the disclosure of over a half million records accounts for 92 percent of all records compromised in Maryland in 2018 (Table 6).

<table>
<thead>
<tr>
<th>Table 6. Top 5 States</th>
<th>As of August 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Rank</td>
</tr>
<tr>
<td>1</td>
<td>CA</td>
</tr>
<tr>
<td>2</td>
<td>TX</td>
</tr>
<tr>
<td>3</td>
<td>MA</td>
</tr>
<tr>
<td>4</td>
<td>IL</td>
</tr>
<tr>
<td>5</td>
<td>FL</td>
</tr>
</tbody>
</table>

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 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](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.


\(^{52}\) OCR conducted 207 desk audits (CEs: 166; BAs: 41). For more information: [cynergistek.com/blog/ocr-desk-audits-preliminary-results/](cynergistek.com/blog/ocr-desk-audits-preliminary-results/).

## All Maryland Breaches

2017

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

### Top 10 Health Care Data Breaches 2017

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

Maryland Breaches by Covered Entity Type

% (N=28)

<table>
<thead>
<tr>
<th>Year</th>
<th>Healthcare Provider</th>
<th>Business Associate</th>
<th>Health Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>50</td>
<td>17</td>
<td>33</td>
</tr>
<tr>
<td>2015</td>
<td>39</td>
<td>63</td>
<td>100</td>
</tr>
<tr>
<td>2016</td>
<td></td>
<td></td>
<td>88</td>
</tr>
<tr>
<td>2017</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend:
- Healthcare Provider
- Business Associate
- Health Plan
Appendix D

Nation Breaches by Covered Entity Type
%  
(N=1,246)

<table>
<thead>
<tr>
<th>Year</th>
<th>Healthcare Provider</th>
<th>Business Associate</th>
<th>Health Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>13</td>
<td>25</td>
<td>62</td>
</tr>
<tr>
<td>2015</td>
<td>23</td>
<td>4</td>
<td>73</td>
</tr>
<tr>
<td>2016</td>
<td>16</td>
<td>6</td>
<td>78</td>
</tr>
<tr>
<td>2017</td>
<td>14</td>
<td>6</td>
<td>80</td>
</tr>
</tbody>
</table>
### Top 10 States Ranking Records Compromised 2017

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

For a listing of all states ranked by population size, visit: [simple.wikipedia.org/wiki/List_of_U.S._states_by_population](simple.wikipedia.org/wiki/List_of_U.S._states_by_population).
## Appendix F

### All Maryland Breaches 2018

<table>
<thead>
<tr>
<th>Organization</th>
<th>Records Compromised</th>
<th>Type of Breach</th>
<th>Covered Entity Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>LifeBridge Health, Inc</td>
<td>538,127</td>
<td>Hacking/IT Incident</td>
<td>Healthcare Provider</td>
</tr>
<tr>
<td>Capital Digestive Care, Inc.</td>
<td>17,639</td>
<td>Unauthorized Access/Disclosure</td>
<td>Healthcare Provider</td>
</tr>
<tr>
<td>Special Agents Mutual Benefit Association</td>
<td>13,942</td>
<td>Unauthorized Access/Disclosure</td>
<td>Health Plan</td>
</tr>
<tr>
<td>CareFirst BlueCross BlueShield</td>
<td>6,200</td>
<td>Hacking/IT Incident</td>
<td>Health Plan</td>
</tr>
<tr>
<td>Westminster Ingleside King Farm Presbyterian Retirement Communities, Inc.</td>
<td>5,228</td>
<td>Hacking/IT Incident</td>
<td>Healthcare Provider</td>
</tr>
<tr>
<td>Serene Sedation, LLC</td>
<td>5,207</td>
<td>Hacking/IT Incident</td>
<td>Healthcare Provider</td>
</tr>
<tr>
<td>StatCare Group LLC</td>
<td>679</td>
<td>Hacking/IT Incident</td>
<td>Healthcare Provider</td>
</tr>
</tbody>
</table>
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 submission 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: THIS SIC 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 acronym)
* 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.
FOR EXTERNAL USE: HIS/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:

FOR EXTERNAL USE: HIS/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 Claims
  • 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 Claims
  • Healthcare Provider
* Street Address Line 1:
  Street Address Line 2:
  * City:
  * State: — Choose State —
  * ZIP:
FOR EXTERNAL USE: HIPAA BREACH REPORT, REQUIRED INFORMATION

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):

Usage

FOR EXTERNAL USE: HIPAA BREACH REPORT, REQUIRED INFORMATION

- Home/Cell
- Work

Breach Information Section

Breach Affecting: How many individuals are affected by the breach?
- 300 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: HIPAA BREACH REPORT: REQUIRED INFORMATION

☐ Network Server
☐ Other Portable Electronic Device
☐ Paper/Files
☐ 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
    □ Claim Information
    □ Credit Card/Health Ins #
    □ Other Financial Information
    □ Other

* Type of Protected Health Information Involved in Breach (Other):
  [1,000 characters limit]

* Brief Description of the Breach:
  [1,000 characters limit]

* Safeguards in Place Prior to Breach:
  □ None
  □ Privacy Rule Safeguards (Training, Policies and Procedures, etc.)
  □ Security Rule Administrative Safeguards (Access Controls, Transmission Security, etc.)

FOR EXTERNAL USE: HIPAA 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 Summary

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

* Individual Notice Provided Start Date:
* Individual Notice Provided Expected End Date:

Was Substantive Notice Required?
  • Yes
  □ Fewer than 180 days
  □ 180 days or more
  • No

Was Media Notice Required?
  • Yes
    □ Select Time and Date when media notice was provided:
      – Time:
      – Date:
    • No

* Actions Taken in Response to Breach:
  □ Adapted encryption technologies
  □ Changed passwords/stronger password requirements
  □ Updated/deleted Security Risk Management Plan
  □ Implemented new technical safeguards
  □ Implemented periodic technical and non-technical evaluations
  □ Improved physical security
  □ Performed new/updated Security Risk Analysis
  □ Provided business associate with additional training on HIPAA requirements
  □ Provided individuals with live credit monitoring
  □ Revised business associate contracts:
  □ Revised policies and procedures
  □ Sanctioned workforce members involved (including termination)
FOR EXTERNAL USE: HHS OCHRED REPORT: REQUIRED INFORMATION

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

ATTENTION Information Sheet

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 1, 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((a)(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(c) 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