Health Care Data Breaches

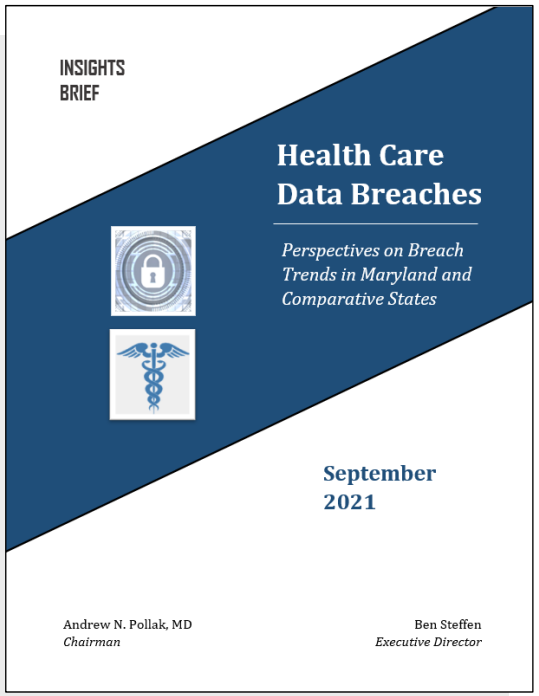
Perspectives on Breach Trends

MARYLAND HEALTH CARE COMMISSION

September 23, 2021

DRAFT

Overview



- Staff conducted a review of breaches reported by covered entities (CEs) and business associates (BAs) from January 1, 2018 to December 31, 2020
  - Data on breaches affecting 500 or more records obtained from the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR)
- Assessed breach trends for:
  - Eight states, including Maryland, (IL, IN, MD, MS, NV, RI, OK, VA) with similar hospital inpatient days (within 10%) per 100,000* population (see Table 1)
  - Other states (remaining 42 states and DC)

**Three consecutive years of data 2017-2019.*

Note: Breaches reported based on headquarter location of CE and BA; breach year represents the date a breach was reported to OCR and may be different than the breach occurrence date.

Current State of Health Care Cybersecurity

- Breaches are due to the evolving nature of cyber threats
  - Threats: criminal financial scammers and nation-states
  - Bad actors are exploiting vulnerabilities from changing circumstances
- Health care organizations (organizations) continue to enhance their security posture
  - Securing data is essential; organizations must remain vigilant
  - Cyber risk management – a key component of a broader business strategy

Findings

Breach Growth, A Snapshot of 2018 – 2020

- ***Occurrences:*** An increase in breaches reported (18% eight states | 35% other states)
- ***Records:*** Compromised records grew similarly among the eight states and other states (45% eight states | 46% other states)
- ***Type:*** Largest growth in hacking/IT incidents, the leading breach type (43% eight states | 66% other states); disproportional growth in records (4% eight states | 69% other states)

**Breach growth calculated using compound annual growth rate (CAGR), a measure of growth over a specified period longer than one year.*

Business Associates

- ***Occurrences*:** Negative growth among the eight states (-6%); other states increased (40%) (see Tables 2-4)
  - Approximately two-thirds (63% eight states | 66% other states) attributed to hacking/IT, the highest percentage across all CE types
- ***Records*:** Considerably higher growth among the eight states (117%), more than four times other states (25%) (see Tables 2-4)
  - Attributed to a breach event* reported in 2020, accounting for about 85% of records for the eight states; at least nine organizations were affected, including two Maryland-based BAs
- Largest breach nationally compromised up to 25 million records resulting from a hacking incident on a billing services vendor (American Medical Collection Agency) – discovered in 2019, eight months after the ransomware attack began
  - Resulted in multiple breach reports, including Optum (MN | 11.5 million records), LabCorp (NC | 10.2 million records), and others

**Cyber-attack was initiated through a phishing email impersonating a Magellan Health client.*

Health Plans

- ***Occurrences*:** Slight growth among the eight states (4%); other states increased (19%) (see Tables 2-4)
  - About half of occurrences (53% eight states | 51% other states) stem from unauthorized access/disclosure
- ***Records*:** Negative growth among the eight states (-54%); other states increased (16%) (see Tables 2-4)
  - Among the eight states, the largest breach compromised nearly 3 million records after a cyber-attack initiated in 2010 was identified and reported in 2019 by Dominion National (VA)

Providers

- ***Occurrences*:** Moderate growth among the eight states (28%) and other states (37%) (see Tables 2-4)
  - Hacking/IT incidents most prevalent (58% eight states | 62% other states)
- ***Records*:** Significant growth among all states (80% eight states | 82% other states) (see Tables 2-4)
  - In 2020, a ransomware attack on a cloud software company (Blackbaud) affected up to 10 million records across more than two dozen providers (including at least five in the eight states)

Breach Type

- Hacking/IT incidents account for the largest share of breaches (57% eight states | 60% other states) and records (90% eight states | 91% other states)
    - Attributed to 9 of the 10 largest breaches reported for the eight states; records compromised range from 111,000 to 3 million (see Table 5)

Addressing Cybersecurity Threats

- Cybersecurity frameworks* help organizations manage, mitigate, and reduce cyber risks
  - Increasingly, organizations are requiring vendors to obtain privacy and security certifications or accreditations to ensure safeguards exceed what is minimally required by HIPAA
- Operating under the assumption that a breach is inevitable improves security preparedness and response to incidents
- In 2020, there was an average of 816 attempted cyber-attacks per end point, a 9,851% increase from the prior year

**Cybersecurity frameworks are comprised of industry guidelines, standards, and best practices developed across multiple disciplines, industries, government, and academia. NIST and HITRUST are among some of the leading frameworks that assist organizations in maintaining compliance and improving cybersecurity preparedness.*

Breach Risks Associated with Patient Generated Health Data

Overview

- Patient generated health data (PGHD) is health-related data created and recorded by or from patients or family members/caregivers outside of a clinical setting using a range of direct-to-consumer health technologies (or "third-party applications")
  - Use of third-party applications is a rapidly growing sector that presents unique pathways to help consumers meet health goals and expand providers' knowledge about patients outside of clinical encounters
  - Supplementing EHR information with PGHD enables a more comprehensive view of a patient's current and ongoing health
- Increasing breach awareness and strengthening privacy and security protections for PGHD is essential to reduce the risk of unauthorized access and cyber threats

Current Landscape

- Privacy and security protections differ across consumer health device vendors that maintain and transmit PGHD; in most instances, PGHD is not protected by HIPAA
  - HIPAA only extends protections to protected health information (PHI) created, received, or maintained by or on behalf of CEs and BAs
  - PGHD presents a new class of PHI about consumers such as who they are, what they do, how healthy they are, what movements they make, and how well they feel
- Third-party applications that lack HIPAA-equivalent privacy and security protections can result in selling or sharing users' data without their consent or knowledge and they can respond differently to a breach
- A need exists to ensure PGHD is adequately safeguarded (includes de-identifying data) and to educate consumers and providers about PHI outside of a HIPAA-regulated environment

Activities on the Horizon

PGHD Awareness Building

- Stakeholder education:
  - Staff plans to develop consumer materials on PGHD and work with select stakeholders to develop a PGHD privacy and security assessment guide aimed at broadening use of third-party applications through sound and evidence-based privacy and security practices

Assess the need for legislation:

  - Staff plans to explore whether legislation as opposed to policy is necessary to strengthen PGHD protections

Cybersecurity Education

- Virtual symposium this fall in collaboration with HSCRC, the Maryland Hospital Association, MD HIMSS, and the Health Facilities Association of Maryland
  - Target audience: hospital and nursing home leadership
  - Theme: mitigating cybersecurity risk across the health care supply chain
- A webinar is planned for ambulatory practices in early 2022
  - Presentations will focus on cybersecurity best practices and overview cyber-related exposures, factors that determine premiums for cyber liability coverage, and the types of coverage available

Data Tables

Table 1: Cohort Quartile Ranking, Breaches Per 100,000, and Other Demographics						
Breach Occurrences 2018-2020	**Cohort**	**Breach Occurrences per 100,000** 2018-2020	**Records per 100,000** 2018-2020	**US Population** 2019	**Physicians** Total 2020 / per 100,000	**Hospitals** Total 2018 / per 100,000
Quartile 1	**RI**	0.57	3,601	1,059,361	5,326 / 503	11 / 1.0
	MS	0.24	2,936	2,976,149	6,679 / 224	99 / 3.3
Quartile 2	**OK**	0.20	7,219	3,956,971	9,609 / 243	125 / 3.1
	NV	0.42	6,729	3,080,156	6,223 / 202	44 / 1.4
Quartile 3	**VA**	0.37	49,861	8,535,519	23,539 / 276	96 / 1.1
	IN	0.52	25,259	6,732,219	16,979 / 252	132 / 1.9
Quartile 4	**MD**	0.66	18,653	6,045,680	25,146 / 416	50 / 0.8
	IL	0.47	9,613	12,671,821	44,100 / 348	187 / 1.4
	Total	3.46	123,870	45,057,876	137,601 / 2,464	744 / 14.3
	Average	0.43	15,484	5,632,235	17,200 / 305	93 / 1.6

US population data obtained from US Census Bureau; physician and hospital data obtained from Kaiser Family Foundation. Quartile is a statistical measure that divides data observations into four equal quarters based on the values of the data, ordered from smallest to largest, to measure the spread of values above and below the mean (average).

Table 2: CAGR by CE Type, 2018-2020						
	Business Associate		Health Plan		Provider	
	Occurrences	Records	Occurrences	Records	Occurrences	Records
Nation	32%	25%	16%	5%	36%	82%
Cohort	-6%	117%	4%	-54%	28%	80%
Other States	40%	25%	19%	16%	37%	82%
Breaches reported by health care clearinghouses are not represented in the table above; the cohort did not experience such breaches in this time period. A dash or (-) signifies a decrease.						

Table 3: Breach Occurrences by CE Type									
	Business Associate			Health Plan			Provider		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
IL	6	2	1	3	6	3	10	13	16
IN	0	2	0	2	3	2	3	8	15
MD	0	3	5	2	1	3	7	11	8
MS	0	0	0	0	1	1	3	2	0
NV	1	0	0	0	0	0	5	5	2
OK	0	0	0	1	0	1	1	4	1
RI	0	0	0	3	0	0	0	2	1
VA	2	0	2	0	2	2	6	4	14
***Total** Cohort*	9	7	8	11	13	12	35	49	57
Other States	33	46	65	41	46	58	237	343	444
Nation	42	53	73	52	59	70	272	392	501

Table 4: Records by CE Type									
	Business Associate			Health Plan			Provider		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
IL	10,164	6,024	917	9,290	35,028	105,036	71,546	87,620	892,483
IN	0	58,110	0	585,537	35,135	3,296	4,553	205,726	808,135
MD	0	57,138	82,523	20,142	87,400	16,289	568,912	43,088	252,230
MS	0	0	0	0	2,000	759	33,981	50,642	0
NV	3,758	0	0	0	0	0	10,257	175,924	17,324
OK	0	0	0	813	0	1,112	279,865	2,271	1,076
RI	0	0	0	8,267	0	0	0	8,588	21,289
VA	4,294	0	2,694	0	2,968,278	7,766	22,051	29,651	1,221,124
***Total** Cohort*	18,216	121,272	86,134	624,049	3,127,841	134,258	991,165	603,510	3,213,661
Other States	5,962,210	12,387,404	9,330,733	2,173,617	247,705	2,930,192	4,116,660	22,343,259	13,660,443
Nation	5,980,426	12,508,676	9,416,867	2,797,666	3,375,546	3,064,450	5,107,825	22,946,769	16,874,104

Table 5: Ten Largest Breaches in the Cohort, 2018-2020				
State	**Organization**	**Records**	**Breach Type**	**CE Type**
VA	Dominion Dental Services Inc. Dominion National Insurance	2,964,778	Hacking/IT Incident	Health Plan
VA	Inova Health System	1,045,270	Hacking/IT Incident	Provider
IN	CNO Ace	566,217	Hacking/IT Incident	Health Plan
IN	Elkhart Emergency Physicians, Inc.	550,000	Improper Disposal	Provider
MD	LifeBridge Health, Inc.	538,127	Hacking/IT Incident	Provider
IL	Northshore University Health System	348,746	Hacking/IT Incident	Provider
OK	Oklahoma State University	279,865	Hacking/IT Incident	Provider
IL	Amita Health	261,054	Hacking/IT Incident	Provider
NV	Laboratory Medicine Consultants, LTD.	140,590	Hacking/IT Incident	Provider
IN	Meridian Health Services Corp.	111,372	Hacking/IT Incident	Provider