HEALTH CARE DATA BREACH TRENDS

2018-2021

October 2022

OVERVIEW

A health care data breach (breach) is the illegitimate access or disclosure of protected health information (PHI).[1, 2] Breaches are commonly classified as internal or external. An internal breach compromises PHI by way of insider threats that can be intentional or unintentional (e.g., privilege abuse, improper disposal, unintended sharing to an unauthorized party); an external breach is caused by an external entity or source (e.g., hacking/IT related incidents, including malware, ransomware, phishing).[3] Evolving cyberattacks, notably ransomware, continue to create a challenging health care cyber threat landscape.[4] Prevention strategies and cyber resiliency are essential to protect PHI, maintain operations, and ensure patient safety.[5]

The Health Information Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, requires covered entities[6] (CE) and business associates[7] (BA) to report a breach of unsecured PHI to the U.S. Department of Health and Human Services (HHS), Office of Civil Rights (OCR).[8, 9] OCR makes select data on breaches affecting 500 or more individuals available through a public use file, including entities that reported a breach, number of records compromised,[10] and breach type.[11]

APPROACH

The Maryland Health Care Commission conducted an analysis of health care data breaches locally and nationally affecting 500 or more individuals.[12] The analysis includes breaches reported to OCR from January 1, 2018 to December 31, 2021.[13] A cohort of eight states was identified based on similarity of hospital inpatient days per 100K.[14, 15, 16] The cohort includes Illinois (IL), Indiana (IN), Maryland (MD), Mississippi (MS), Nevada (NV), Oklahoma (OK), Rhode Island (RI), and Virginia (VA). Findings provide insights into breach trends and the changing cybersecurity landscape.

The following summary is intended to build awareness of breaches and foster dialogue regarding approaches to risk management and the implementation and maintenance of cybersecurity best practices. The information that follows illustrates breach data for the nation and cohort,[17] including notable observations regarding breach trends and characteristics that call to light the importance of cybersecurity preparedness, risk mitigation, and incident response capabilities.

OVERALL TRENDS

Table 1a. Breach Snapshot										
	Breach Occurrences				Records				Total / CAGR	
	2018	2019	2020	2021	2018	2019	2020	2021	Breach Occurrences	Records
Nation (All States)	367	505	662	714	14,120,003	40,465,581	34,308,610	45,744,177	2,248 / 25%	134,638,371 / 48%
Cohort (Eight States)	55	68	77	119	1,633,430	3,858,974	4,327,319	5,894,214	319 / 29%	15,713,937 / 53%
Other States (Excludes Cohort)	312	437	585	595	12,486,573	36,606,607	29,981,291	39,849,963	1,929 / 24%	118,924,434 / 47%

Table 1b. Cohort Totals by State										
Cohort	Breach Occurrences				Records				Total / CAGR	
	2018	2019	2020	2021	2018	2019	2020	2021	Breach Occurrences	Records
IL	19	20	20	41	91,000	130,214	998,435	1,874,767	100 / 29%	3,094,416 / 174%
IN	5	13	17	16	590,090	303,280	813,015	1,626,344	51 / 47%	3,332,729 / 40%
MD	9	15	16	15	589,054	187,626	1,237,712	311,592	55 / 19%	2,325,984 / -19%
MS	3	3	1	8	33,981	52,642	759	82,647	15 / 39%	170,029 / 35%
NV	6	5	2	9	14,015	175,924	17,324	1,473,638	22/ 15%	1,680,901 / 372%
OK	2	4	2	11	280,678	2,771	2,188	258,948	19 / 77%	544,585 / -3%
RI	3	2	1	4	8,267	8,588	26,234	11,904	10 / 10%	54,993 / 13%
VA	8	6	18	15	26,345	2,997,929	1,231,652	254,374	47 / 23%	4,510,300 / 113%
Total	55	68	77	119	1,633,430	3,858,974	4,327,319	5,894,214	319 / 29%	15,713,937 / 53%
Average	6.9	8.5	9.6	14.9	204,179	482,372	540,915	736,777	39.9 / 29%	1,964,242 / 53%

Notes: A dash or (-) signifies a decrease; compound annual growth rate (CAGR) is a measure of growth for multiple time periods

Year-over-year growth in breaches has slowed; records have increased[18]

Nationally, breaches continue to increase (Table 1a); however, growth rate in reported breaches has decreased since 2018:[19] 38 percent (2018 to 2019), 31 percent (2019 to 2020), 8 percent (2020 to 2021).[20] Unrelenting cyberattacks involve millions of records each year, which can sometimes be attributed to a single breach. For example, an unauthorized user gained access to internal systems at American Medical Collection Agency for several months and compromised over 13M records, representing about 86 percent of records reported across five states in 2019.[21] LabCorp was one of nine provider organizations impacted and represents the largest share of records compromised (about 10M).[22] In 2020, ransomware impacted MD-based US Fertility, LLC with 50 clinics throughout the nation; this breach is responsible for the sharp increase in records, compromising nearly 900K or about 71 percent of records reported that year for MD (Table 1b).[23]

A CLOSER LOOK AT THE COHORT

Table 2. Cohort Quartile Ranking, Breaches Per 100,000, and Other Demographics

Breach Occurrences 2018-2021	Cohort	Breach Occurrences per 100,000 2018-2021	Records per 100,000 2018-2021	US Population 2020	Physicians Total 2022 / per 100,000	Hospitals Total 2020 / per 100,000
Quartile 1	RI	0.91	5,011	1,097,379	5,663 / 516	11 / 1.0
	MS	0.51	5,742	2,961,279	6,954 / 235	97 / 3.3
Quartile 2	OK	0.48	13,754	3,959,353	9,922 / 251	122 / 3.1
	NV	0.71	54,142	3,104,614	6,442 / 207	46 / 1.5
Quartile 3	VA	0.54	52,255	8,631,393	25,234 / 292	95 / 1.1
	IN	0.75	49,115	6,785,528	17,339 / 256	129 / 1.9
Quartile 4	MD	0.89	37,654	6,177,224	25,802 / 418	49 / 0.8
	IL	0.78	24,152	12,812,508	45,739 / 357	184 / 1.4
Total		5.57	241,825	45,529,278	143,095 / 2,532	733 /14.1
Average		0.70	30,228	5,691,160	17,887 / 316	92 / 1.8

Notes: 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); states in the cohort are ranked based on total number of breach occurrences from 2018-2021

State size is not an indicator of breach impact

Some less populous states in the cohort had more breach occurrences per capita (Table 2). For example, RI had the least amount of breach occurrences (10) from 2018 to 2021 with four or less reported each year (Table 1b). Four breaches reported by CVS, a chain headquartered in the state, involved pharmacy locations nationwide. One breach was due to vandalism that resulted in roughly 26K records being compromised, nearly half of records for RI from 2018 to 2021 (Table 1b).[24] NV, ranking fifth in the cohort with 22 breach occurrences (Table 1b), reported the most records per capita (Table 2). A 2021 breach compromised 1.3M records (about 77 percent of records reported in NV from 2018-2021) after a hospital became victim of Russian hacking group ReVIL.[25] ReVIL was responsible for around 73 percent of ransomware detection globally (across all sectors) in the second quarter of 2021.[26]

BREACHES BY ENTITY TYPE

Table 3. CAGR by Entity Type, 2018-2021						
	Business Associates		Health Plans		Providers	
	Occurrences	Records	Occurrences	Records	Occurrences	Records
Nation	30%	21%	24%	36%	24%	74%
Cohort	33%	164%	22%	-16%	31%	74%
Other States	30%	20%	25%	45%	32%	74%

Notes: Breaches reported by health care clearinghouses are not represented in the table above; the cohort did not experience such breaches in this period; a dash or (-) signifies a decrease

Third party vulnerabilities broadly impact CEs

Health care operations supported by BAs have generally experienced more growth in breach occurrences (Table 3). In 2021, three states in the cohort (RI, OK, and MS) had BAs report breaches (a total of five all combined) for the first time since 2018 (Table 5a in Appendix). Steep growth in records for BAs in the cohort (Table 3) can be attributed to two states (IL and VA),[27] which reported the most breach occurrences in 2021 (a total of 12 combined), accounting for nearly 80 percent of records (Tables 5a and 5b in Appendix). Providers continue to report the vast majority of breaches to OCR (roughly 75 percent of breaches from 2018-2021), prompting the Federal Bureau of Investigation to issue several special warnings in collaboration with HHS and the Cybersecurity and Infrastructure Security Agency.[28] A BA breach can impact multiple providers that often submit separate reports to OCR.[29] For example, a ransomware attack on Elekta, a radiology software company, affected approximately 170 health care organizations nationwide,[30] including locations in three cohort states (IL, NV, and OK).[31] The breach delayed or disrupted treatment for cancer patients and compromised about 274K records in the cohort.

BREACH TYPE

Table 4. CAGR by Breach Type, 2018-2021										
	Hacking/IT		Improper Disposal		Loss		Theft		Unauthorized Access/Disclosure	
	Occurrences	Records	Occurrences	Records	Occurrences	Records	Occurrences	Records	Occurrences	Records
Nation	47%	62%	-21%	-18%	-8%	4%	-16%	-46%	2%	-8%
Cohort	58%	57%					-11%	9%	-11%	-18%
Other States	45%	63%	-26%	-19%	-12%	2%	-18%	-49%	4%	-7%

Notes: The cohort did not report breaches due to loss in 2018 or improper disposal in 2018 and 2019. A dash or (-) signifies a decrease.

Hacking trends persist with phishing being the most common

Hacking/IT incidents continue to account for the vast majority of breach occurrences (74 percent) and records (94 percent) in 2021 (Tables 6a and 6b in Appendix). For the cohort, hacking/IT incidents more than doubled in 2021; MD and VA were the only states to not experience an increase (Table 6a). Rate of growth overall for hacking/IT incidents has slowed in the nation: 46 percent (2018 to 2019), 32 percent (2019 to 2020), 14 percent (2020 to 2021) (Table 6a).[32] Phishing is the most common point of compromise for about 71 percent of hacking/IT incidents.[33] American Anesthesiology reported one of the largest breaches of 2021 (nearly 1.27M records) after phishing compromised the email system of its BA (MEDNAX).[34] Other breach types reported to OCR consist of unauthorized access/disclosure (about 20 percent),[35] and theft, loss, and improper disposal (all of which account for less than 5 percent of breach occurrences).

CONCLUSION

Breach trends demonstrate that money motivates bad actors to acquire PHI, which is the most valued type of data to compromise.[36, 37] For the health care industry, cyberattacks that rely on ransomware for potential monetary gain have almost doubled, increasing from 34 percent in 2020 to 66 percent in 2021.[38] More than half (61 percent) of health care organizations pay a ransom,[39] the highest of all industries. Though it's generally recommended that organizations under attack not pay a ransom,[40] the potential risk to patient health and safety makes the decision much harder for health care organizations because it's often a faster way to restore operations and ensure continuity of services.[41] Hospitals are frequent targets of ransomware as bad actors understand the critical need to access patient data, and any period in which the electronic health record is unavailable is operationally disruptive.[42]

The health care industry continues to embrace a culture of privacy and security as electronic PHI is created, stored, and utilized. Securely maintaining this flow of PHI, while also ensuring authorized access to the data, is paramount to mitigate risks that could endanger patients and cause operational, financial, and regulatory challenges. Data encryption[43] is part of a layered approach to cybersecurity (e.g., firewalls[44])[45] and ranks third among 20 factors that can mitigate the cost of a breach.[46] Advances in data encryption have made cyberattacks less likely to succeed, making it a key component of a data protection strategy. Lessons learned from breaches inform how CEs and BAs evolve policies and procedures for safeguarding PHI. These experiences inform risk management practices to protect the health care supply chain and reduce the impact of a breach.[47]

LIMITATIONS

Breaches are reported based on the state where the entity is headquartered, but the entity may operate in other states. Breach year represents the date a breach was reported to OCR and may be different than the breach occurrence date.[48] Specific information related to origin of the breach, cause, and type of patient information compromised is not available for all breach reports.[49]

RESOURCES

MHCC Cybersecurity Web Page – A collection of links to cybersecurity webinars, tools, and educational materials, including resources for small health care practices

HHS 405(d) Aligning Health Care Industry Security Approaches Program – Resources and best practices to help mitigate and respond to cyber threats

American Medical Association: Physician Cybersecurity – Guidance for safeguarding confidential and patient information in a medical practice

APPENDIX

Table 5a. Breach Occurrences by CE Type, 2018-2021

	Business Associate				Health Plan				Provider			
	2018	2019	2020	2021	2018	2019	2020	2021	2018	2019	2020	2021
IL	8	2	1	9	3	6	3	8	10	12	16	24
IN	0	2	0	2	2	3	2	7	3	8	15	7
MD	0	3	5	2	2	1	3	1	7	11	8	12
MS	0	0	0	1	0	1	1	0	3	2	0	7
NV	1	0	0	0	0	0	0	1	5	5	2	8
OK	0	0	0	3	1	0	1	1	1	4	1	7
RI	0	0	0	1	3	0	0	1	0	2	1	2
VA	2	0	2	3	0	2	2	1	6	4	14	11
Total *Cohort*	9	7	8	21	11	13	12	20	35	48	57	78
Other States	33	47	66	72	43	46	60	84	238	343	457	437
Nation	42	54	74	93	54	59	72	104	273	391	514	515

Table 5b. Records by CE Type, 2018-2021

	Business Associate				Health Plan				Provider			
	2018	2019	2020	2021	2018	2019	2020	2021	2018	2019	2020	2021
IL	10,164	6,024	917	170,023	9,290	35,028	105,035	252,550	71,546	89,162	892,483	1,452,194
IN	0	58,110	0	7,508	585,537	35,135	3,380	35,677	4,553	210,035	809,635	1,583,159
MD	0	57,138	966,050	54,825	20,142	87,400	16,289	500	568,912	43,088	255,373	256,267
MS	0	0	0	501	0	2,000	759	0	33,981	50,642	0	82,146
NV	3,758	0	0	0	0	0	0	45,000	10,257	175,924	17,324	1,428,638
OK	0	0	0	4,883	813	0	1,112	868	279,865	2,771	1,076	253,197
RI	0	0	0	3,064	8,267	0	0	5,015	0	8,588	26,234	3,825
VA	4,294	0	2,694	95,776	0	2,968,278	7,740	33,932	22,051	29,651	1,221,218	124,666
Total *Cohort*	18,216	121,272	969,661	336,580	624,049	3,127,841	134,315	373,542	991,165	609,861	3,223,343	5,184,092
Other States	5,979,057	13,012,859	11,286,480	10,256,445	2,209,922	247,708	3,767,322	10,219,483	4,333,899	24,619,115	14,941,457	22,978,849
Nation	5,997,273	13,134,131	12,256,141	10,593,025	2,833,971	3,375,549	3,901,637	10,593,025	5,325,064	25,228,976	18,164,800	28,162,941

Table 6a. Occurrences by Breach Type, 2018-2021

	Hacking/IT Incident				Improper Disposal				Loss			
	2018	2019	2020	2021	2018	2019	2020	2021	2018	2019	2020	2021
IL	6	10	9	31	0	0	0	1	0	1	0	1
IN	4	9	9	14	0	0	7	0	0	0	0	0
MD	5	11	13	13	0	0	0	0	0	0	0	0
MS	1	1	0	7	0	0	0	0	0	0	0	0
NV	2	2	1	7	0	0	0	0	0	1	0	0
OK	2	2	1	9	0	0	1	0	0	1	0	0
RI	0	1	0	1	0	0	0	0	0	0	1	0
VA	4	4	16	13	0	0	1	0	0	0	0	0
***Total** Cohort*	24	40	49	95	0	0	9	1	0	3	1	1
Other States	141	268	405	433	10	6	7	4	13	12	13	9
Nation	165	308	454	528	10	6	16	5	13	15	14	10

	Theft				Unauthorized Access/Disclosure			
	2018	2019	2020	2021	2018	2019	2020	2021
IL	4	1	1	1	9	8	10	7
IN	1	0	0	1	0	4	1	1
MD	1	1	0	1	3	3	3	1
MS	0	1	0	0	2	1	1	1
NV	0	1	0	0	4	1	1	2
OK	0	1	0	1	0	0	0	1
RI	0	1	0	1	3	0	0	2
VA	1	0	0	0	3	2	1	2
***Total** Cohort*	7	6	1	5	24	19	17	17
Other States	34	31	38	19	114	120	122	130
Nation	41	37	39	24	138	139	139	147

Table 6b. Records by Breach Type, 2018-2021

	Hacking/IT Incident				Improper Disposal				Loss			
	2018	2019	2020	2021	2018	2019	2020	2021	2018	2019	2020	2021
IL	64,906	61,498	888,855	1,836,153	0	0	0	6,498	0	811	0	1,352
IN	588,659	193,374	255,529	1,608,851	0	0	554,876	0	0	0	0	0
MD	555,441	167,025	1,224,477	307,534	0	0	0	0	0	0	0	0
MS	1,670	30,642	0	82,146	0	0	0	0	0	0	0	0
NV	4,221	144,669	16,622	1,470,690	0	0	0	0	0	27,004	0	0
OK	280,678	1,050	1,112	251,776	0	0	1,076	0	0	500	0	0
RI	0	2,943	0	5,015	0	0	0	0	0	0	26,234	0
VA	15,978	2,992,987	1,223,012	248,657	0	0	7,983	0	0	0	0	0
Total *Cohort*	1,511,553	3,594,188	3,609,607	5,810,822	0	0	563,935	6,498	0	28,315	26,234	1,352
Other States	8,700,683	35,601,359	26,660,595	37,363,492	342,272	26,081	21,045	184,042	29,966	45,956	31,589	32,006
Nation	10,212,236	39,195,547	30,270,202	43,174,314	342,272	26,081	584,980	190,540	29,966	74,271	57,823	33,358

	Theft				Unauthorized Access/Disclosure			
	2018	2019	2020	2021	2018	2019	2020	2021
IL	6,572	1,600	72,143	777	19,522	66,305	37,437	29,987
IN	1,431	0	0	5,505	0	109,906	2,610	11,988
MD	1,310	679	0	1,553	32,303	19,922	13,235	2,505
MS	0	20,000	0	0	32,311	2,000	759	501
NV	0	2,251	0	0	9,794	2,000	702	2,948
OK	0	1,221	0	6,134	0	0	0	1,038
RI	0	5,645	0	826	8,267	0	0	6,063
VA	2,100	0	0	0	8,267	4,942	657	5,717
Total *Cohort*	11,413	31,396	72,143	14,795	110,464	205,075	55,400	60,747
Other States	673,707	328,629	740,151	91,594	2,739,945	604,582	2,527,911	2,178,829
Nation	685,120	360,025	812,294	106,389	2,850,409	809,657	2,583,311	2,239,576

Endnotes

[1] PHI may include information that is demographic (e.g., name, e-mail, date of birth, social security number, etc.), financial (e.g., service dates, payment method, etc.), or clinical (e.g., diagnoses, prescriptions, treatment, etc.).
[2] Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, Khan RA. Healthcare Data Breaches: Insights and Implications. Healthcare (Basel). 2020 May 13;8(2):133. doi: 10.3390/healthcare8020133. PMID: 32414183; PMCID: PMC7349636.
[3] *Ibid.*
[4] Ransomware is a type of malicious software, or malware, that withholds access to computer files, systems, or networks while demanding payment.
[5] MedCity News, *Protecting Hospitals from Evolving Cyber Threats*, September 2022. Available at: medcitynews.com/2022/05/protecting-hospitals-from-evolving-cyber-threats/.
[6] CEs include health plans, health care clearinghouses, health care providers, and business associates. More information is available at: www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html.
[7] BAs include entities that create, receive, maintain, or transmit PHI on behalf of a CE or another BA.
[8] CEs and BAs must notify OCR within 60 days from discovery of a breach affecting more than 500 individuals; breaches affecting fewer than 500 individuals must be reported within 60 days of the end of the calendar year. More information is available at: www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html.
[9] BAs are also required to notify CEs upon discovery of a breach.
[10] Instances may exist where it cannot be determined exactly how records have been breached; CEs and BAs err on the side of caution and report the entire database for records compromised.
[11] Breach type includes hacking/IT incident, improper disposal, loss, theft, unauthorized access/disclosure, unknown, and other.
[12] Details on breaches affecting fewer than 500 records are not published by OCR.
[13] Data was obtained from an OCR public use file available at: ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
[14] States within 10 percent of Maryland hospital inpatient days make up the cohort. States with greater inpatient days per capita include IL, NV, OK, RI; states with fewer inpatient days per capita include IN, MS, VA.
[15] Data represent 2017-2019 and was obtained from the American Hospital Association Annual Survey, which uses a consistent definition and reporting methodology. More information is available at: www.kff.org/other/state-indicator/inpatient-days-by-ownership/?currentTimeframe=0&sortModel=%7B%22colId%22:%22Location%22,%22sort%22:%22asc%22%7D.
[16] This approach accounted for state-level differences in population size and the utilization of hospital care, which is related to and affected by changes in population characteristics and market forces. Using crude rate permits comparisons of populations that differ in size; however, this approach does not consider variables such as demographic characteristics that may affect the observed rate. More information is available at: www.paho.org/english/sha/EB_v23n3.pdf.
[17] See n. 14-16, *Supra*.
[18] In general, there is more fluctuation (increases and decreases) in reported records.
[19] Calculated using percent change, the difference between an old and new value.
[20] Year-over year growth in reported breaches: Cohort – 24 percent (2018 to 2019), 13 percent (2019 to 2020), 35 percent (2020 to 2021); Other states – 29 percent (2018 to 2019), 34 percent (2019 to 2020), 2 percent (2020 to 2021).
[21] States affected by the American Medical Collection Agency breach include California (564,642 records), New Jersey (583,766 records), New York (1,183,629 records), North Carolina (10,219,786 records), and Texas (2,453,984 records).
[22] Fierce Healthcare, *Number of Patient Records Breached Nearly Triples in 2019,* February 2020. Available at: www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats.
[23] Health IT Security, *US Fertility Sued Over Ransomware Attack, Health Data Exfiltration*, February 2021. Available at: healthitsecurity.com/news/us-fertility-sued-over-ransomware-attack-health-data-exfiltration.
[24] CVS Pharmacy reported vandalism at stores in several states between May 27 and June 8, 2020, which resulted in the loss of some patient information. More information is available at: www.beckershospitalreview.com/cybersecurity/cvs-pharmacy-data-breach-affects-21-289-patients.html.
[25] Becker's Health IT, *Hackers Hit Las Vegas Hospital, Steal Data and Post Online: 5 Details*, June 2021. Available at: www.beckershospitalreview.com/cybersecurity/hackers-hit-las-vegas-hospital-steal-data-and-post-online-5-details.html.
[26] Health IT Security, *73% of Ransomware Detections in Q2 2021 Credited to REvil/Sodinokibi*, October 2021. Available at: healthitsecurity.com/news/73-of-ransomware-detections-in-q2-2021-credited-to-revil-sodinokibi.
[27] Four of the occurrences for the cohort were reported by the same accounting firm around one incident – a 2020 ransomware attack that resulted in late notification of affected individuals. More information is available at: www.hipaajournal.com/december-2021-healthcare-data-breach-report/.
[28] Cybersecurity & Infrastructure Security Agency, *Nation Cyber Awareness System > Alerts*. Available at: www.cisa.gov/uscert/ncas/alerts.
[29] Protenus, *2022 Breach Barometer*. Available at: www.protenus.com/breach-barometer-report.
[30] Becker's Health IT, *Elekta Software Breach Hits Advocate Aurora, Intermountain; 96,000 Patients Affected*, July 2021. Available at: www.beckershospitalreview.com/cybersecurity/elekta-software-breach-hits-advocate-aurora-intermountain-96-000-patients-affected.html.

[31] Providers in the cohort impacted by the ransomware attack on Elekta include Renown Healthcare (NV), Cancer Centers of Southwest Oklahoma (OK), and Northwestern Memorial Healthcare (IL).
[32] See n. 19, *Supra*.
[33] Healthcare Information and Management Systems Society, *2021 HIMSS Healthcare Cybersecurity Survey*, 2022. Available at: www.himss.org/sites/hde/files/media/file/2022/01/28/2021_himss_cybersecurity_survey.pdf.
[34] Healthcare IT News, *The Biggest Healthcare Data Breaches of 2021*, November 2021. Available at: www.healthcareitnews.com/news/biggest-healthcare-data-breaches-2021.
[35] Providers reported 80 percent of unauthorized access/disclosure incidents for the cohort in 2021; examples of 2021 breaches involving unauthorized access/disclosure breaches include an IL county health department emailing vaccination reminders to 800 patients without using the blind carbon copy function, a misconfigured database that exposed PHI through a public-facing portal in VA, and a former OK hospital employee accidentally donating items to charity that contained handwritten notes with patient names, ages, diagnoses, and medications.
[36] Fierce Healthcare, *Industry Voices—Forget Credit Card Numbers. Medical Records Are the Hottest Items on the Dark Web*, January 2021. Available at: www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web#:~:text=Cybersecurity%20firm%20Trustwave%20pegged%20the,as%20little%20as%20%241%20each.
[37] Researchers have a limited understanding of the amount PHI sells for on the dark web. Some estimate a health care record could sell for $250; based on this estimate, ransomware that compromises 1,000 records could be worth about $250,000. More information is available at: www.copycei.com/ransomware-in-healthcare/.
[38] Sophos, *The State of Ransomware in Healthcare 2022*, June 2022. Available at: news.sophos.com/en-us/2022/06/01/the-state-of-ransomware-in-healthcare-2022/.
[39] The average ransom amount in health care is $197,000, which is much lower than the average cost of $812,000 across all industry sectors. More information is available at: www.hipaajournal.com/healthcare-ransomware-attacks-increased-by-94-in-2021/#:~:text=While%20the%20healthcare%20industry%20had,all%20industry%20sectors%20was%20%24812%2C000.
[40] The FBI and Department of Homeland Security recommend not paying a ransom. Whether or not to pay a ransom is more nuanced in a health care setting since continuity is critical and could be a matter of life and death. More information is available at: www.healthcareitnews.com/news/ransomware-attacks-pay-or-not-pay.
[41] Cyberpeace Institute, *Ransomware Against Healthcare: To Pay or Not to Pay?* December 2021. Available at: cyberpeaceinstitute.org/news/ransomware-against-healthcare-to-pay-or-not-to-pay/.
[42] Verizon, *How Data Encryption Protects Patients*. Available at: www.verizon.com/business/resources/articles/s/how-data-encryption-protects-patients/.
[43] Encryption is a way of encoding data in a complex way so only authorized parties can receive and understand the information. Unencrypted data can be manipulated and go undetected.
[44] A firewall is one of the first lines of defense that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
[45] See n. 42, *Supra*.
[46] IBM, *How Much Does a Data Breach Cost in 2022?* July 2022. Available at: www.ibm.com/security/data-breach?_ga=2.84355353.164459074.1661437525-961019030.1658239877.
[47] The health care supply chain is an extensive network of systems, components, and processes that collectively work to ensure medicines and other healthcare supplies are manufactured, distributed, and provided to patients. More information is available at: healthcareready.org/what-is-the-healthcare-supply-chain/.
[48] Breach event lifecycle involves the occurrence (when the incident happened), discovery (when an organization becomes aware of the incident), and notification (date the initial notification was provided).
[49] Breaches currently under investigation do not include this information.