INSIGHTS
BRIEF

Health Care Data Breaches

Perspectives on Breach Trends in Maryland and Comparative States

September 2021

Andrew N. Pollak, MD
Chairman

Ben Steffen
Executive Director

MARYLAND HEALTH CARE COMMISSION

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

Bimbola Akintade, PhD
University of Maryland School of Nursing
Associate Professor for the School of Nursing

Arun Bhandari, MD
Chesapeake Oncology Hematology
Associates, PA

Cassandra Boyer, BA
Business Operations Manager
Enterprise Information Systems Directorate
US Army Communications Electronics Command

Marcia Boyle, MS
Founder
Immune Deficiency Foundation

Trupti N. Brahmbhatt, PhD
Senior Policy Researcher
Rand Corporation

Tinisha Cheatham, MD
Physician in Chief of the Mid-Atlantic
Permanente Medical Group

Martin L. "Chip" Doordan, MHA
Retired Chief Executive Officer
Anne Arundel Medical Center

Jeffrey Metz, MBA, LNHA
President and Administrator
Egle Nursing and Rehab Center

Gerard S. O'Connor, MD
General Surgeon in Private Practice

Michael J. O'Grady, PhD
Principal, Health Policy LLC, and
Senior Fellow, National Opinion Research Ctr
(NORC) at the University of Chicago

Martha G. Rymer, CPA
Rymer & Associates, PA

Randolph S. Sergent, Esq
Vice Chair, Maryland Health Care Commission
Vice President and Deputy General Counsel
CareFirst BlueCross BlueShield

Stephen B. Thomas, PhD
Professor of Health Services Administration
School of Public Health
Director, Maryland Center for Health Equity
University of Maryland, College Park

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

Table of Contents

Introduction

An increase of health care breaches is due to an evolving cyber threat landscape.[1] Ransomware[2] and phishing[3] are the most rampant forms of cybercrime that rely on human error to carry out a cyber-attack. Cybersecurity is a crucial component in health care, particularly amid the COVID-19 public health emergency (PHE).[4, 5] Safeguarding health information technology (health IT) is a data, systems, and patient safety issue.[6, 7] Managing cyber risks requires offensive measures that prevent exploitation or misuse of systems that support care delivery (e.g., medical devices, electronic health record or EHR systems, hardware, and software).[8] Risks are calculated based on the likelihood and impact of potential threats, and inform cybersecurity approaches that balance the need to provide uninterrupted care and properly protect data and systems.[9] Key components to mitigating cyber risk include end point management, security awareness, incident response, and business continuity planning.[10] Strong policies and procedures are the underpinnings to protecting critical assets, timely detect compromises, and respond to incidents effectively.[11]

Purpose, Approach, and Limitations

The Maryland Health Care Commission (MHCC) conducted an analysis of health care data breaches locally and nationally affecting 500 or more individuals.[12] The analysis included breach reports submitted to the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) from January 1, 2018 to December 31, 2020 by covered entities[13] (CEs) and business associates[14] (BAs).[15, 16] Data was obtained from the OCR public use file[17] and contains information on breach occurrences, breach type,[18] and records potentially[19] compromised. Findings provide insight into breach trends and the changing cybersecurity landscape to improve approaches to risk management and the implementation of cybersecurity best practices related to preparedness, prevention, and response.

The analysis includes Maryland and seven other states[20] that were identified based on similarity of hospital inpatient days per 100,000 for three years (2017-2019).[21] 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.[22] States within 10 percent of Maryland's hospital inpatient days[23] make up the cohort (eight states in total).[24]

Breaches are reported based on the state where the entity is headquartered; entities subject to this review may operate in Maryland and other states, including the comparison cohort. Breach year represents the date a breach was reported to OCR and may be different than the breach occurrence date.[25] Specific information related to origin of the breach, cause, and type of patient information compromised is not available for all breach reports.[26]

Findings

A Snapshot of Reported Breaches

Greater volatility exists in the magnitude of reported records compared to occurrences. Between 2018 and 2020, approximately 82 million records were breached nationally; individual states reported a range of 1,260 (SD) to 13,745,539 (NC) total records (Appendix A). Breach occurrences for the cohort increased at about half the rate (18 percent CAGR[27]) as compared to other states (35 percent CAGR) (Table 1a). Four states within the cohort experienced declines or no growth in breach occurrences (Missouri, Nevada, Oklahoma, and Rhode Island); three states had declines in records reported (Maryland, Missouri, Oklahoma) (Table 1b).

Table 1a. Overall Totals

	Breach Occurrences			Records			Total (Compound Annual Growth Rate or CAGR)	
	2018	2019	2020	2018	2019	2020	Breach Occurrences	Records
Nation (All States)	367	505	646	13,893,013	38,849,591	29,406,640	1,518 (33%)	82,149,244 (46%)
Cohort (8 States)	55	69	77	1,633,430	3,853,123	3,434,053	201 (18%)	8,922,106 (45%)
Other States (Excludes Cohort)	312	436	569	12,259,583	34,996,468	25,966,600	1,317 (35%)	73,227,138 (46%)

Table 1b. Cohort Totals by State

Cohort	Breach Occurrences			Records			Total (CAGR)	
	2018	2019	2020	2018	2019	2020	Breach Occurrences	Records
IL	19	21	20	91,000	128,672	998,436	60 (3%)	1,218,108 (231%)
IN	5	13	17	590,090	298,971	812,931	35 (84%)	1,701,992(17%)
MD	9	15	16	589,054	187,626	351,042	40 (33%)	1,127,722 (-23%)
MS	3	3	1	33,981	52,642	759	7 (-42%)	87,382 (-85%)
NV	6	5	2	14,015	175,924	17,324	13 (-42%)	207,263 (11%)
OK	2	4	2	280,678	2,771	2,188	8 (0%)	285,637 (-91%)
RI	3	2	1	8,267	8,588	21,289	6 (-42%)	38,144 (60%)
VA	8	6	18	26,345	2,997,929	1,231,584	32 (50%)	4,255,858 (584%)
Total	55	69	77	1,633,430	3,853,123	3,435,553	201 (18%)	8,922,106 (45%)
Average	7	9	10	204,179	481,640	429,444	25 (18%)	1,115,263 (45%)

Note: A dash or (-) signifies a decrease.

Improving Security Posture

Health care organizations (organizations) leverage cybersecurity frameworks[28] comprised of industry guidelines, standards, and best practices developed across multiple disciplines, industries, government, and academia. Cybersecurity frameworks help organizations manage, mitigate, and reduce cyber risks. The National Institute of Standards and Technology and the Health Information Trust Alliance (HITRUST) have developed frameworks to assist organizations in maintaining compliance and improving cybersecurity preparedness (Appendix B).[29]

Examining the Cohort – An Overall Summary of the Population Experience

States that are more populous generally report more breaches. Illinois, Indiana, Maryland, and Virginia have larger populations and comprise the third and fourth (or highest) quartiles for occurrences. These states have about the same or more than the cohort average for total physicians (17,200) and hospitals (93) except for Maryland, which has less hospitals (roughly half) than the cohort average. Rhode Island, which accounts for the smallest population and total physicians and hospitals, has the second largest number of breaches per capita. Maryland has a higher number of breaches per capita than other states in the cohort (Table 2).

Table 2. Cohort Quartile[30] Ranking, Breaches Per 100,000[31], 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

Notes: US population data obtained from US Census Bureau; physician and hospital data obtained from Kaiser Family Foundation.

Raising Cybersecurity Awareness

As organizations evolve their cybersecurity policies and procedures, their efforts to increase and reinforce awareness of cybersecurity expand in parallel. Routine training improves understanding of the critical role cybersecurity plays in day-to-day operations and helps organizations of all sizes establish a culture of data privacy and security.[32] Well-designed, organization-wide processes and personnel training that incorporate continued engagement and realistic security exercises promote higher levels of security awareness among staff.[33] Optimizing training requires ongoing review and revision of training approaches and materials as new training techniques develop and new threats appear.

Breaches by Covered Entity Type

Breach occurrences have increased among BAs in other states in the cohort (2018: 33, 2019: 46, 2020: 65) impacting multiple providers and records reported (Tables 3c and 3d). Breach occurrences reported by BAs in the cohort have remained relatively consistent, experiencing a modest decline of six percent between 2018 and 2020, compared to a 40 percent increase in the other states (Table 3a). BAs in the cohort reported the largest growth for records (117 percent), more than four times the growth in other states (Table 3a). The increase is largely due to a single breach in 2020 involving 72,970 records, accounting for about 85 percent of all records[34] reported by BAs (eight total breaches) (Table 3d). The breach resulted from a cyber-attack initiated through a phishing email impersonating a Magellan Health client. At least nine organizations nationally were affected, including two Maryland-based BAs.[35]

Breach occurrences reported by health plans experienced moderate increases whereas providers had greater increases year over year (Table 3c)**; records reported had much more variability** (Table 3d)**.** Occurrences reported by providers between 2018 and 2020 increased for the cohort (28 percent) and other states (37 percent) (Table 3a). Providers account for a little over half of all records reported by CE types (54 percent cohort; 55 percent other states[36]) (Table 3b). A cyber-attack experienced by a single health plan in Virginia (Dominion National) accounts for about 70 percent of all records reported for the state.[37] Breaches at health plans tend to involve higher number of records due to the large volumes of protected health information (PHI) held by health plans.[38]

Table 3a. 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%

Notes: 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 3b. Breaches by CE Type, Totals 2018-2020

	Occurrences				Records			
	Business Associate	Health Plan	Provider	Combined Total	Business Associate	Health Plan	Provider	Combined Total
IL	9	12	39	60	17,105	149,354	1,051,649	1,218,108
IN	2	7	26	35	58,110	623,968	1,018,414	1,700,492
MD	8	6	26	40	139,661	123,831	864,230	1,127,722
MS	0	2	5	7	0	2,759	84,623	87,382
NV	1	0	12	13	3,758	0	203,505	207,263
OK	0	2	6	8	0	1,925	283,212	285,137
RI	0	3	3	6	0	8,267	29,877	38,144
VA	4	4	24	32	6,988	2,976,044	1,272,826	4,255,858
Total *Cohort*	24	36	141	201	225,622	3,886,148	4,808,336	8,920,106
Other States	144	145	1,024	1,313	27,680,347	5,351,514	40,120,362	73,152,223
Nation	168	181	1,165	1,514	27,905,969	9,237,662	44,928,698	82,072,329

Table 3c. 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 3d. 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

Note: Refer to Table 3b for totals by covered entity type and all combined.

Managing Third-Party Risk

Nationally, an average of 1,320 third-party vendors (vendors) provide services (e.g., billing, data storage, claims processing, practice management, etc.) to larger organizations.[39] To reduce the risk of a breach, expectations are communicated to vendors in business associate agreements (BAA)[40] and contracts.[41] Increasingly, organizations are requiring vendors to obtain privacy and security certifications or accreditations to ensure safeguards exceed what is minimally required by Health Insurance Portability and Accountability Act of 1996 (HIPAA)[42] as amended by the Health Information Technology for Economic and Clinical Health Act in 2009.[43, 44] CEs' and BAs' security policies define screening processes to identify vendors listed on federal or state sanction lists before entering into a BAA or contract, as well as a requirement to conduct annual reviews of vendors' independent security audit reports.[45]

Breach Types

External cyber threats (e.g., malware) and insider-related threats (e.g., negligence/human error or malicious wrongdoing) dominate breach trends.[46] These threats are growing in sophistication, volume, and frequency, resulting in breaches where external threats generally outpace insider-related threats.[47, 48] Hacking/IT incidents experienced the largest growth between 2018 and 2020 (cohort: 43 percent, other states: 66 percent) (Table 4c). During this time, hacking/IT accounted for over 50 percent of breach occurrences (57 percent cohort; 60 percent other states[49]) and records (88 percent cohort; 91 percent other states[50]) reported to OCR during this period (Tables 4a and 4b). Nine of the 10 largest breaches in the cohort are due to hacking/IT incidents and collectively total 6.8 million records (range: 111,000 to three million records, see Appendix C).

Improper physical safeguards (i.e., security measures, policies, and procedures) result in disposal and theft of paper records and electronic media. In 2020, improper disposal accounted for the largest share of records for the cohort of states. Multiple breach reports from providers in Indiana were the result of an improper method used by a BA to dispose of 554,876 paper records (Table 4b).[51] Paper medical records and billing statements containing names, contact information, social security numbers, dates of services, and clinical and diagnostic information were recovered at a dumping site.[52] Breaches resulting from theft declined in the cohort from seven occurrences in 2018 to one in 2020 (Table 4d). Theft accounts for about one percent of records for the cohort (Table 4b); however, one breach contributed to theft experiencing significant growth (151 percent) between 2018 and 2020 (Table 4c). This breach was reported by Walgreens (based in Illinois) and involved a series of break-ins at 180 pharmacies throughout the nation in May and June 2020 impacting 72,143 records.[53] Paper records and computer hard drives were among the items stolen.[54]

Table 4a. Occurrences by Breach Type, Totals 2018-2020

	Hacking/IT Incident	Improper Disposal	Loss	Theft	Unauthorized Access/ Disclosure	Combined Total
IL	26	0	1	6	27	60
IN	22	7	0	1	5	35
MD	29	0	0	2	9	40
MS	2	0	0	1	4	7
NV	5	0	1	1	6	13
OK	5	1	1	1	0	8
RI	1	0	1	1	3	6
VA	24	1	0	1	6	32
Total *Cohort*	114	9	4	14	60	201
Other States	790	32	39	103	362	1,326
Nation	904	39	43	117	422	1,525

Table 4b. Records Compromised by Breach Type, Totals 2018-2020

	Hacking/IT Incident	Improper Disposal	Loss	Theft	Unauthorized Access/ Disclosure	Combined Total
IL	1,013,717	0	811	80,315	123,265	1,218,108
IN	1,033,169	554,876	0	1,431	112,516	1,701,992
MD	1,060,273	0	0	1,989	65,460	1,127,722
MS	32,312	0	0	20,000	35,070	87,382
NV	165,512	0	27,004	2,251	12,496	207,263
OK	282,840	1,076	500	1,221	0	285,637
RI	2,943	0	21,289	5,645	8,267	38,144
VA	4,231,909	7,983	0	2,100	13,866	4,255,858
Total *Cohort*	7,822,675	563,935	49,604	114,952	370,940	8,922,106
Other States	66,399,335	389,398	224,142	1,736,745	4,487,845	73,237,465
Nation	74,222,010	953,333	273,746	1,851,697	4,858,785	82,159,571

Table 4c. CAGR by Breach Type, 2018-2020										
	Hacking/IT Incident		Improper Disposal		Loss		Theft		Unauthorized Access/Disclosure	
	Occurrence	Records	Occurrence	Records	Occurrence	Records	Occurrence	Records	Occurrence	Records
Nation	62%	65%	26%	31%	7%	138%	-2%	9%	1%	-47%
Cohort	43%	34%					-62%	151%	-16%	-29%
Other States	66%	69%	-16%	-75%	4%	122%	6%	4%	5%	-48%
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.										

Table 4d. Occurrences by Breach Type									
	Hacking/IT Incident			Improper Disposal			Loss		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
IL	6	11	9	0	0	0	0	1	0
IN	4	9	9	0	0	7	0	0	0
MD	5	11	13	0	0	0	0	0	0
MS	1	1	0	0	0	0	0	0	0
NV	2	2	1	0	0	0	0	1	0
OK	2	2	1	0	0	1	0	1	0
RI	0	1	0	0	0	0	0	0	1
VA	4	4	16	0	0	1	0	0	0
Total *Cohort*	24	41	49	0	0	9	0	3	1
Other States	140	266	384	10	6	16	13	12	14
Nation	164	307	433	10	6	23	13	15	15

	Theft			Unauthorized Access/Disclosure		
	2018	2019	2020	2018	2019	2020
IL	4	1	1	9	8	10
IN	1	0	0	0	4	1
MD	1	1	0	3	3	3
MS	0	1	0	2	1	1
NV	0	1	0	4	1	1
OK	0	1	0	0	0	0
RI	0	1	0	3	0	0
VA	1	0	0	3	2	1
Total *Cohort*	7	6	1	24	19	17
Other States	34	31	38	115	121	126
Nation	41	37	39	139	140	143

Note: Refer to Table 4b for occurrence totals by breach type and all combined.

Table 4e. Records by Breach Type									
	Hacking/IT Incident			Improper Disposal			Loss		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
IL	64,906	59,956	888,855	0	0	0	0	811	0
IN	588,659	189,065	255,445	0	0	554,876	0	0	0
MD	555,441	167,025	337,807	0	0	0	0	0	0
MS	1,670	30,642	0	0	0	0	0	0	0
NV	4,221	144,669	16,622	0	0	0	0	27,004	0
OK	280,678	1,050	1,112	0	0	1,076	0	500	0
RI	0	2,943	0	0	0	0	0	0	21,289
VA	15,978	2,992,987	1,222,944	0	0	7,983	0	0	0
Total *Cohort*	1,511,553	3,588,337	2,722,785	0	0	563,935	0	28,315	21,289
Other States	8,480,887	33,582,649	24,335,799	342,272	26,081	21,045	29,966	45,956	148,220
Nation	9,992,440	37,170,986	27,058,584	342,272	26,081	584,980	29,966	74,271	169,509

	Theft			Unauthorized Access/Disclosure		
	2018	2019	2020	2018	2019	2020
IL	6,572	1,600	72,143	19,522	66,305	37,438
IN	1,431	0	0	0	109,906	2,610
MD	1,310	679	0	32,303	19,922	13,235
MS	0	20,000	0	32,311	2,000	759
NV	0	2,251	0	9,794	2,000	702
OK	0	1,221	0	0	0	0
RI	0	5,645	0	8,267	0	0
VA	2,100	0	0	8,267	4,942	657
Total *Cohort*	11,413	31,396	72,143	110,464	205,075	55,401
Other States	673,707	328,629	734,409	2,741,896	1,014,335	731,614
Nation	685,120	360,025	806,552	2,852,360	1,219,410	787,015

Note: Refer to Table 4c for record totals by breach type and all combined.

Strengthening Resilience

On average, organizations take about 103 days to contain a breach.[55] Operating under the assumption that a breach is inevitable improves organizations' response to security incidents and equips them to address incidents with greater speed and precision.[56] Incident response plans (IRPs) provide detailed guidance for responding to security incidents and are adaptive to meet unique needs that satisfy legal requirements, serve patients, and minimize reputational damage.[57] Organizations typically evolve their IRPs in parallel with the threat landscape.[58] A well thought out IRP considers a range of worst case scenarios (e.g., outsider presence within the network, denial of service) and develops protocols accordingly to help organizations identify, eliminate, and recover from a security incident.[59, 60]

Discussion

Bolstering security posture is mission critical in health care and key to reducing the breach risk. Persistent threats come from nation states and criminal financial scammers (scammers).[61, 62] Attacks by nation-states and scammers have increased in prevalence and sophistication, and typically rely on techniques that interrupt business operations, leak confidential information, and compromise large volumes of data.[63] Ransomware is the prominent root cause of breaches, accounting for almost half (46.4 percent) of all breaches in 2020; other leading causes include email compromise (24.6 percent), insider threat (7.3 percent) and application misconfiguration (5.6 percent).[64, 65]

In 2020, health care sector accounted for the largest share of breaches (24.5 percent)[66] across all industries.[67] Cyber-attacks in the health care sector more than doubled[68] as threat actors targeted victims with malware and phishing campaigns using COVID-19 as a lure (e.g., masquerading as the World Health Organization and requesting payments). In March 2020, the health care sector received about 16 percent more malicious emails than any other sector.[69] Overall, cyber-attacks against health care organizations consisted of large and small-scale cybercrime linked to 35 unique threat actors (e.g., criminal enterprises. scammers, nation-states, etc.).[70] In about 90 percent of incidents involving email compromise the subject line was blank, a strong marker for targeted security detection and focused user awareness training.[71]

Cyber-attacks can potentially have a profound impact on operations and patient care. Cybersecurity compounded the challenges some organizations faced in responding to the COVID-19 PHE. Roughly 250 hospitals nationally experienced a ransomware attack in 2020, blocking access to systems for an average of three weeks.[72] Medical records were rendered temporarily inaccessible and, in some cases, permanently lost. At times, ambulances had to be rerouted and radiation treatments for patients delayed.[73] The U.S. Cybersecurity and Infrastructure Security Agency issued an advisory[74] to health care organizations in October 2020 warning of the increased risk of ransomware.[75]

A robust risk management approach considers all systems that could expose PHI and assets that could impact the safe delivery of patient care.[76] The interconnectivity of technology systems yields multiple end points, increasing the likelihood that a security vulnerability could be exploited.[77] Threat actors target these end points: networks, records disposal, remote work, data storage, internet of things (which includes medical devices, among others[78]), and personal devices.[79, 80] In 2020, an average of 816 attempted cyber-attacks per end point was reported, a 9,851 percent increase from the prior year.[81] Reducing end point security gaps, with particular attention on third-parties and supply chain risks, is essential.[82] This requires knowing where devices are, what software applications are installed, and what known vulnerabilities exist.[83]

Building and maintaining a strong security culture is critical for organizations.[84] Adopting security automation technologies results in faster and more cost-effective incident detection and response. Automation technologies help reduce the estimated cost of a breach by half as compared to when the technologies are not in place (i.e., $2.45 million compared to $6.03 million, on average).[85] Beyond investments in technology, cultivating an information security culture enables organizations to better prepare for and respond to a breach and any regulatory investigation that follows.[86] Conducting periodic training for employees on best practices for security and compliance raises awareness of existing policies and procedures.

Building Cybersecurity Awareness: A Key Role for MHCC

The MHCC is planning a cybersecurity symposium for hospital and nursing home leadership in fall 2021. The symposium will be convened in collaboration with the HSCRC, the Maryland Hospital Association, MD HIMSS, and the Health Facilities Association of Maryland. Discussions will center on best practices for securing supply chain systems and points of potential vulnerability.

A cybersecurity webinar is planned for small ambulatory practices in early 2022. Presentations will highlight cyber liability insurance to protect practices from costs associated with a cyber-attack or data breach. The webinar will overview cyber-related exposures, factors that determine premiums for cyber liability coverage (e.g., volume of patient records, existing practice controls, etc.), and the types of coverage available.[87]

The MHCC previously convened symposiums and hosted webinars on cybersecurity. These events provide opportunities for stakeholders to share perspectives and best practices on cybersecurity and discuss technologies and processes that support a strategic and anticipatory risk-based approach to cybersecurity.

Looking Ahead: Breach Risks Associated with Patient Generated Health Data

What is Patient Generated Health Data?

Patient generated health data (PGHD) is defined as health-related data created and recorded by or from patients or family members/caregivers outside of a clinical setting.[88] PGHD is distinct from clinical data generated in a health care setting in that someone other than a treating provider records the data and decides whether to share the data with providers and other third parties.[89, 90] Supplementing existing EHR information with PGHD enables a more comprehensive view of a patient's current and ongoing health, such as how the patient is doing in-between provider visits. PGHD can help identify changes in a patient's condition or symptoms, prompting a different approach to treatment.[91, 92] Benefits also include empowering consumers to better manage their health and participate in their care, which can strengthen the patient-provider relationship through shared decision-making.[93]

To reduce the risk of cyber threats and unauthorized access to PGHD, health care organizations and policymakers must increase awareness and strengthen privacy and security protections. Health developers have important roles in implementing strong security protections that will instill confidence in patients and providers. Capturing, using, and sharing PGHD is made possible by a wide range of direct-to-consumer health technologies. This rapidly growing sector presents unique pathways to help consumers meet health goals and expand providers' knowledge about patients outside of clinical encounters, particularly for those with chronic conditions.[94, 95] PGHD can be integrated into provider workflows and EHR systems, helping to improve diagnosis and treatment.[96] Privacy and security protections vary across consumer health devices that maintain or transmit PGHD. In most instances, PGHD is not protected by HIPAA as amended by HITECH.[97] Some states are beginning to explore or pass legislation to ensure minimum safeguards for PGHD that falls outside the scope of HIPAA.[98, 99]

Current Landscape

Health technology companies that sell consumer health devices, such as sensors and wearables (also referred to as "third-party applications"), offer many health tracking capabilities (e.g., heart rate, respirations, temperature, steps per day, glucose level, and location tracking, among other things) that enable select aspects of health to be managed from anywhere, at any time.[100] Nationally, approximately 43 percent[101] of patient

portals tethered to an EHR system[102] accept PGHD.[103, 104] Patient portals managed by CEs and BAs are responsible for protecting PGHD and preventing a data breach.[105] HIPAA, the most far-reaching federal health care law in the United States, only extends protections to PHI created, received, or maintained by or on behalf of CEs and BAs.[106] PHI loses its protected status after being disclosed to a third-party application at a consumer's discretion.[107, 108] These third-party applications lack HIPAA-equivalent privacy and security protections,[109] which can result in selling or sharing users' data without their consent or knowledge and responding to a breach differently.[110]

Third-party applications continue to be embraced by consumers, increasing privacy and security risks at an alarming pace.[111] All 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have breach notification laws with provisions on who must comply (e.g., private or government entities); how personal information is defined (e.g., name combined with SSN, driver's license or state ID, account numbers, and health information); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice and who must be notified); and exemptions (e.g., if information is encrypted).[112] Approximately 22 states (including Maryland) have breach notification laws that include health information in their definition of personal information.[113] At the federal level, the Health Breach Notification Rule[114] requires entities not covered by HIPAA (i.e., personal health record vendors and related entities) to inform consumers about unauthorized disclosures of PHI.[115] The Federal Trade Commission (FTC) is tasked with enforcement of the Health Breach Notification Rule[116] to protect consumers when PGHD is misused.

Key Concerns

PGHD derived from third-party applications presents a new class of data about consumers such as who they are, what they do, how healthy they are, what movements they make, and how well they feel.[117] Third-party applications that are not subject to HIPAA pose serious challenges in protecting PHI. At issue is whether PGHD is adequately safeguarded and if consumers are aware of and understand what privacy rights they have in regards to their electronic health information.[118, 119] Concerns also exist around steps taken by third-party applications to adequately de-identify PGHD.[120] The likelihood of reidentifying such data increases when inadequate security measures are in place.[121] The Office of the National Coordinator for Health Information Technology (ONC) has expressed concerns about the possibility of reidentifying de-identified data from third-party applications.[122, 123]

Next Steps

Increase privacy and security awareness of PGHD among providers and consumers.

Greater awareness of the privacy and security risks and development of best practices associated with PGHD are essential to bolstering consumer protections and use of the data in care delivery.[124, 125] Educating stakeholders on appropriate safeguards, including privacy and security policies, supports greater utility of PGHD for clinical purposes in the future.[126] Migration of PHI outside of the HIPAA-regulated environment is expected to accelerate in part due to federal interoperability rules[127] relating to consumer-facing applications,[128] and the move away from fee-for-service reimbursement to new payment and care delivery models.[129, 130] The MHCC plans to develop consumer education material on PGHD and work with stakeholders to develop a provider PGHD privacy and security assessment guide that includes clinical, regulatory, and technical considerations. These initiatives aim to broaden awareness and use of third-party applications guided by sound and evidence-based privacy and security practices.[131]

Explore the need for legislation to align PGHD safeguards with HIPAA.

Companies offering third-party applications often lack ample privacy and security protections that are equivalent to those required by HIPAA.[132] Implementation of consistent physical and technical safeguards through statute can reduce existing and emerging risks related to PGHD.[133] Notably, PGHD was not considered by Congress when HIPAA was established 25 years ago.[134] Nationally, stakeholders (including the American Medical Informatics Association and American Health Information Management Association) have lobbied to address uneven protections among third-party applications, encouraging HHS and Congress to propose changes to HIPAA.[135] Changes in federal law are not anticipated in the foreseeable future; some states are considering legislation to address privacy and security gaps for this evolving threat landscape.[136] The MHCC plans to explore the impact of legislation (proposed or passed) in other states aimed at strengthening PGHD protections to inform policy development or potential legislation.

Appendix A

Total Breaches, 2018-2020					
State	Occurrences	Records	State	Occurrences	Records
AK	8	69,797	MT	7	172,371
AL	9	502,153	NC	35	13,745,539
AR	27	413,610	ND	2	37,229
AZ	32	1,927,486	NE	12	253,596
CA	129	3,034,487	NH	2	27,615
CO	29	892,143	NJ	25	710,258
CT	34	1,633,136	NM	16	452,558
DC	5	76,320	NV	13	207,263
DE	11	355,318	NY	83	4,000,564
FL	86	5,489,083	OH	63	1,931,872
GA	43	1,663,516	OK	8	285,637
HI	5	50,044	OR	24	892,350
IA	41	1,834,778	PA	67	1,539,087
ID	5	16,471	PR	0	0
IL	60	1,218,108	RI	6	38,144
IN	35	1,701,992	SC	18	396,317
KS	13	174,847	SD	2	1,260
KY	25	457,827	TN	27	1,447,491
LA	14	538,081	TX	133	4,851,324
MA	46	1,158,139	UT	16	675,692
MD	40	1,127,722	VA	32	4,255,858
ME	9	744,299	VT	2	72,982
MI	49	3,802,927	WA	31	2,131,021
MN	54	12,517,542	WI	26	510,994
MO	41	1,984,398	WV	7	15,830
MS	7	87,382	WY	4	24,786
Combined Total	1,518	82,149,244			

Appendix B

Most Used Security Frameworks in Health Care	
Framework	Share (%)
NIST	57.9
HITRUST	26.4
Critical Security Controls	24.7
ISO	18.5
COBIT	7.3
Note: Data obtained from HIMSS 2018 Cybersecurity Survey.	

Appendix C

Ten Largest Breaches, Cohort 2018-2020				
State	**Organization**	**Records**	**Type**	**Covered Entity**
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

Appendix D

Breach Occurrences by Industry, 2020		
#	**Industry**	**Share (%)**
1	Health care	24.5
2	Technology	15.5
3	Education	13.0
4	Government	12.5
5	Entertainment/Food	9.3
6	Finance	7.3
7	Retail	7.3
8	Travel	4.2
9	Manufacturing	3.0
10	Oil/Gas/Energy	1.8
11	Media/News	1.1
Note: Data obtained from HHS Office of Information Security 2020 Retrospective Look at Healthcare Cybersecurity.		

Appendix E

HIPAA and COVID-19

HIPAA established national standards to protect the privacy and security of PHI with the foresight there would be greater digitization of health care data.[137] HITECH amended HIPAA to address a marked shift from paper processes to electronic information systems.[138] In January 2021, Congress amended HITECH to create a safe harbor for health care organizations that have implemented recognized security best practices prior to experiencing a breach.[139] The provision aims to incentivize health care organizations to adopt a recognized cybersecurity framework for regulatory compliance and patient safety. The OCR must consider efforts taken by health care organizations to prevent cyber-attacks when determining penalties.[140]

An outbreak of infectious disease, or other emergency, allows the Secretary of HHS to waive certain sanctions and penalties for noncompliance with specific provisions of the HIPAA Privacy Rule.[141] Following declaration of a PHE due to COVID-19, a limited waiver of HIPAA sanctions and penalties was put in place effective March 15, 2020. The waiver provided flexibility in care delivery by not imposing penalties for noncompliance with certain requirements under HIPAA Rules, including the good faith provision of telehealth services.[142] This permitted use of popular non-public facing audio or video communications products (e.g., Apple FaceTime, Facebook Messenger video chat, etc.) to promote continuation of care delivery. The waiver is in effect for the duration of the PHE.[143] A letter from the Secretary of HHS to state governors in January 2021 advises that the PHE will likely remain in place for the entirety of 2021; states will be provided 60 days' notice when a decision is made to terminate the declaration or let it expire.[144]

[1] Jay G Ronquillo, J Erik Winterholler, Kamil Cwikla, Raphael Szymanski, Christopher Levy, Health IT, Hacking, and Cybersecurity: National Trends in Data Breaches of Protected Health Information, *JAMIA Open*, Volume 1, Issue 1, July 2018, Pages 15–19. Available at: doi.org/10.1093/jamiaopen/ooy019.
[2] Ransomware is a type of malicious software, or malware, that withholds access to computer files, systems, or networks while demanding payment.
[3] Phishing is an attempt to trick a recipient into giving out valuable information (e.g., credentials, insurance information) and is a common way for hackers to deploy ransomware.
[4] He Y, Aliyu A, Evans M, Luo C. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review [published correction appears in J Med Internet Res. 2021 Apr 28;23(4):e29877]. *J Med Internet Res.* 2021;23(4):e21747. Published 2021 Apr 20. Available at: www.ncbi.nlm.nih.gov/pmc/articles/PMC8059789/.
[5] See Appendix E for information about HIPAA, including waivers implemented in response to the PHE.
[6] BACS, *Safe Harbor Laws: Mitigating the Impact of a Data Breach,* May 2021. Available at: bacsit.com/2021/05/17/safe-harbor-laws-mitigating-the-impact-of-a-data-breach/.
[7] American Hospital Association Center for Health Innovation, *The Importance of Cybersecurity in Protecting Patient Safety.* Available at: www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety.
[8] Healthcare and Public Health Sector Partnership, *Healthcare and Public Health Cybersecurity Primer: Cybersecurity 101.* Available at: www.phe.gov/Preparedness/planning/cip/Documents/cybersecurity-primer.pdf.
[9] See n. 6, *Supra.*
[10] See n. 4, *Supra.*
[11] Harvard Business Review, *Make Your Organization More Resilient to Cyber Attacks,* April 2021. Available at: hbr.org/sponsored/2021/04/make-your-organization-more-resilient-to-cyber-attacks.
[12] Details on breaches affecting fewer than 500 records are not published by OCR.
[13] 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.
[14] BAs include entities that create, receive, maintain, or transmit PHI on behalf of a CE or another BA.
[15] 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.
[16] BAs are also required to notify CEs upon discovery of a breach.
[17] The OCR breach portal is available here: ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
[18] Breach type includes hacking/IT incident, improper disposal, loss, theft, unauthorized access/disclosure, unknown, and other.
[19] Instances exist where it may be challenging to determine what records within a database have been breached; CEs and BAs often err on the side of caution and report the entire database for records compromised.
[20] Cohort includes: IL, IN, MD, MS, NV, OK, RI, and VA.
[21] Data is from the American Hospital Association Annual Survey, which uses a consistent definition and reporting methodology. Data for 2020 was not available for this analysis. 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.
[22] Pan American Health Organization, Epidemiological Bulletin, Vol 23, No 3, September 2002. More information is available at www.paho.org/english/sha/EB_v23n3.pdf.
[23] Cohort states with greater patient days per capita (2017-2019) include: IL, NV, OK, RI. Cohort states with fewer patient days per capita include: IN, MS, VA.
[24] 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.
[25] Breach occurrence lifecycle involves occurrence (when the incident happened), discovery (when an organization becomes aware of incident), and notification (date initial notification was provided).
[26] Breaches currently under investigation do not include this information.
[27] CAGR is a measure of growth for multiple time periods.
[28] Cybersecurity frameworks generally undergo periodic reviews and are updated as necessary through additional guidance or supplemental materials to address industry-specific changes and operating environments. More information is available at: us-cert.cisa.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf.
[29] HIMSS, *2018 HIMSS Cybersecurity Survey.* Available at: www.himss.org/sites/hde/files/d7/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf.
[30] 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).
[31] See n. 22, *Supra.*
[32] Cybercrime Magazine, *Healthcare Industry to Spend $125 Billion on Cybersecurity From 2020 to 2025*, September 2020. Available at: cybersecurityventures.com/healthcare-industry-to-spend-125-billion-on-cybersecurity-from-2020-to-2025/.
[33] Small Business Rainmaker, *6 Steps to Promote Cyber Security Awareness in Your Business*, May 2021. Available at: www.smallbusinessrainmaker.com/small-business-marketing-blog/6-steps-to-promote-better-cyber-security-awareness-in-your-business.
[34] Percentage of records reported by BAs in the cohort in 2020: 72,980/86,134*100 = 85 percent. MD BAs: Magellan Healthcare (50,410 records) and National Imaging Associates (22,560 records). Cohort BA records (2020): 86,134.
[35] Maryland-based BAs include Magellan Healthcare and National Imaging Associates.
[36] Percentage of records reported by providers from 2018 to 2020: 4,808,336/8,920,106*100 = 54 percent (cohort); 40,120,362/73,200,055*100 = 55 percent (other states).
[37] HIPAA Journal, *2.9 Million Members Affected by Dominion National 9-Year PHI Breach*, July 2019. Available at: www.hipaajournal.com/dominion-national-discovers-9-year-phi-breach/.
[38] HIPAA Journal, *2020 Healthcare Data Breach Report: 25% Increase in Breaches in 2020*, January 2021. Available at: www.hipaajournal.com/2020-healthcare-data-breach-report-us/.
[39] The Ponemon Institute surveyed 554 health care organizations consisting of health systems, hospitals, clinics, and others. More information is available at: www.censinet.com/ponemon-research-report-the-economic-impact-of-third-party-risk-management-in-healthcare/.
[40] A BAA, as required by HIPAA, establishes the permitted uses and disclosures of PHI, among other things. More information is available at: www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

[41] Healthcare Innovation, *Managing Third-Party Risk,* May 2020. Available at: www.hcinnovationgroup.com/cybersecurity/article/21138595/managing-thirdparty-risk.
[42] Pub. L. 104-191, Aug. 21, 1996, 110 Stat. 1936.
[43] Pub. L. No. 111-5, 123 Stat. 226.
[44] IS Partners, *Time to Talk to Your Business Associates About HITRUST CSF Certification?* October 2020. Available at: www.ispartnersllc.com/blog/hitrust-csf-certification-bas/.
[45] Security Magazine, *Third-Party Risk Management: Keeping your Healthcare Organization's Information Safe*, September 2019. Available at: www.securitymagazine.com/articles/90976-third-party-risk-management-keeping-your-healthcare-organizations-information-safe.
[46] Security Boulevard, *5 Cybersecurity Threats that Will Dominate 2020,* January 2020. Available at: securityboulevard.com/2020/01/5-cybersecurity-threats-that-will-dominate-2020/.
[47] Analytic Exchange Program, *Vulnerabilities of Healthcare Information Technology Systems*, 2018. Available at: www.dni.gov/files/PE/Documents/2018-AEP-Healthcare-Phishing.pdf.
[48] After a four-year decline in insider-related incidents, the health care industry experienced a slight increase in 2020: 2018 (28 percent), 2019 (19 percent), 2020 (20 percent). More information is available at: www.protenus.com/resources/2021-breach-barometer.
[49] Percentage of occurrences due to hacking/IT incidents reported from 2018 to 2020: 114/201*100 = 57 percent (cohort); 790/1,326*100 = 60 percent (other states).
[50] Percentage of records due hacking/IT incidents reported from 2018 to 2020: 7,822,675/8,922,106*100 = 88 percent (cohort); 66,399,335/73,237,465*100 = 91 percent (other states).
[51] The BA, Central File Inc., is an Indiana-based record storage facility. More information is available at: www.databreachtoday.com/business-associate-incidents-added-to-breach-tally-a-14456.
[52] HIPAA Journal, *St Joseph Health System Discovers Medical Record Storage Facility Improperly Disposed of Patient Records*, June 2020. Available at: www.hipaajournal.com/st-joseph-health-system-discovers-medical-record-storage-facility-improperly-disposed-of-patient-records/.
[53] Several other retail pharmacies were targeted (e.g., CVS Pharmacy, Cub Pharmacies) during a period of civil unrest.
[54] Data Breach Today, *Breaches Tied to Pharmacy Looting: Security Lessons,* August 2020. Available at: www.databreachtoday.com/breaches-tied-to-pharmacy-looting-security-lessons-a-14757.
[55] Varonis, *Data Breach Response Times: Trends and Tips,* June 2020. Available at: www.varonis.com/blog/data-breach-response-times/.
[56] Healthcare IT News, *How Provider Organizations can Prepare Cybersecurity Incident Response and Recovery*, November 2019. Available at: www.healthcareitnews.com/news/how-provider-organizations-can-prepare-cybersecurity-incident-response-and-recovery.
[57] Healthcare Information Management Systems Society, *7 Best Practices for a Successful Incident Response Plan,* October 2012. Available at: www.healthcareitnews.com/news/7-best-practices-successful-incident-response-plan.
[58] Health Tech Digital, *Data Breach Response Plan: How Healthcare Providers Should Respond to a Security Incident,* November 2019. Available at: www.healthtechdigital.com/data-breach-response-plan-how-healthcare-providers-should-respond-to-a-security-incident/.
[59] HealthTech, *Why an Incident Response Plan is Necessary for Healthcare Organizations,,* April 2021. Available at: healthtechmagazine.net/article/2021/04/why-healthcare-organizations-need-effective-incident-response-plan.
[60] Security Metrics, *How to Develop and Implement a Successful Incident Response Plan.* Available at: www.securitymetrics.com/learn/how-to-develop-implement-successful-incident-response-plan.
[61] The Wall Street Journal, *Hospitals Suffer New Wave of Hacking Attempts,* February 2021. Available at: www.wsj.com/articles/hospitals-suffer-new-wave-of-hacking-attempts-11612261802?tpl=cybersecurity.
[62] U.S. Department of Health & Human Services, Health Sector Cybersecurity Coordination Center, *2020: A Retrospective Look at Healthcare Cybersecurity*, February 2021. Available at: www.hhs.gov/sites/default/files/2020-hph-cybersecurty-retrospective-tlpwhite.pdf.
[63] Security Magazine, *Concerned about Nation State Cyberattacks? Here's How to Protect your Organization*, March 2020. Available at: www.securitymagazine.com/articles/91889-concerned-about-nation-state-cyberattacks-heres-how-to-protect-your-organization.
[64] See n. 62, *Supra.*
[65] Tenable, *Tenable's 2020 Threat Landscape Retrospective*, January 2021. Available at: www.techdemand.io/whitepaper/security/tenables-2020-threat-landscape-retrospective/.
[66] See n. 62, *Supra.*
[67] See Appendix D for more information on breaches by industry.
[68] Health IT Security, *Healthcare Cyberattacks Doubled in 2020, with 28% Tied to Ransomware*, February 2021. Available at: healthitsecurity.com/news/healthcare-cyberattacks-doubled-in-2020-with-28-tied-to-ransomware.
[69] Proofpoint, *2020 Healthcare Threat Landscape,* December 2020. Available at: www.proofpoint.com/sites/default/files/e-books/pfpt-us-tr-healthcare-report.pdf.
[70] *Ibid.*
[71] See n. 69, *Supra.*
[72] See n. 62, *Supra.*
[73] See n. 62, *Supra.*
[74] Cybersecurity & Infrastructure Security Agency, *Ransomware Activity Targeting the Healthcare and Public Health Sector*, November 2020. Available at: us-cert.cisa.gov/ncas/alerts/aa20-302a.
[75] HIT Consultant, *Why Ransomware Poses a Threat to Both Providers & Patient Health,* May 2021. Available at: hitconsultant.net/2021/05/20/ransomware-healthcare-organizations-patient-health%E2%80%8B/#.YLE6tahKiUk.
[76] CI Security, *Third Party Risk Management for Healthcare Cybersecurity.* Available at: www.ci.security/resources/news/article/third-party-risk-management-for-healthcare-cybersecurity.
[77] Security, *Healthcare Security Challenge: How Cyberattacks are Evolving*, January 2021. Available at: www.securitymagazine.com/articles/94381-healthcare-security-challenge-how-cyberattacks-are-evolving.
[78] From a health care perspective, the internet of things can be considered as any device that can collect health-related data from individuals, including computing devices, mobile phones, smart bands and wearables, digital medications, implantable surgical devices, or other portable devices, which can measure health data and connect to the internet.
[79] See n. 62, *Supra*.
[80] Becker's Health IT, *6 Vulnerability Points Hackers Target in Hospital Cyberattacks,* February 2021. Available at: www.beckershospitalreview.com/cybersecurity/6-vulnerability-points-hackers-target-in-hospital-cyberattacks.html.
[81] See n. 62, *Supra.*
[82] See n. 61, *Supra.*

[83] Absolute, *Endpoint Complexity is Driving Risk Says New Absolute Research*, June 2020. Available at: www.absolute.com/blog/endpoint-complexity-is-driving-risk-says-new-absolute-research/.
[84] Advenica, *Security Culture – An Important Part of Cybersecurity*, January 2020. Available at: advenica.com/en/blog/2020-01-23/security-culture-an-important-part-of-cybersecurity.
[85] Healthcare Innovation, *Report: Healthcare Data Breach Costs Top All Industries Once Again*, July 2020. Available at: www.hcinnovationgroup.com/cybersecurity/data-breaches/news/21148102/report-healthcare-data-breach-costs-top-all-industries-once-again.
[86] Children's Hospital Association, *10 Ways a Hospital Can Prepare and Respond to a Data Breach*, April 2014. Available at: www.childrenshospitals.org/newsroom/childrens-hospitals-today/issue-archive/issues/spring-2014/articles/how-to-prepare-for-and-respond-to-a-data-breach.
[87] Health IT Security, *What is Cyber Insurance for Healthcare Organizations?* February 2019. Available at: healthitsecurity.com/features/what-is-cyber-insurance-for-healthcare-organizations.
[88] ONC, *What are Patient-Generated Health Data?* January 2018. Available at: www.healthit.gov/topic/otherhot-topics/what-are-patient-generated-health-data.
[89] Examples of PGHD include blood glucose monitoring or blood pressure readings using home health equipment, exercise and diet tracking using a mobile application, and questionnaires such as screening, medication adherence, risk assessment, and intake. More information is available at: www.healthit.gov/sites/default/files/patient_generated_data_factsheet.pdf.
[90] Parnassus Consulting, *Patient Generated Health Data Beyond Wearable Devices*. Available at: www.ehcca.com/presentations/pophealthcoll17/foltz_ms4.pdf.
[91] Increasingly, policymakers encourage innovative uses of PGHD through regulatory measures, payment models, and health IT incentives. Use of PGHD has been identified by ONC as an important issue for advancing patient engagement, care delivery, and research. More information is available at: www.healthit.gov/sites/default/files/onc_pghd_final_white_paper.pdf.
[92] National Learning Consortium, *Patient-Generated Health Data, March* 2014. Available at: www.healthit.gov/sites/default/files/patient_generated_data_factsheet.pdf.
[93] American Medical Association, *Why Patients Worry about Cybersecurity and Patient-Generated Data*, February 2019. Available at: www.ama-assn.org/practice-management/digital/why-patients-worry-about-cybersecurity-and-patient-generated-data.
[94] Austin E, Lee JR, Amtmann D, Bloch R, Lawrence SO, McCall D, Munson S, Lavallee DC. Use of Patient-Generated Health Data Across Healthcare Settings: Implications for Health Systems. JAMIA Open. 2019 Nov 29;3(1):70-76. doi: 10.1093/jamiaopen/ooz065. Available at: www.ncbi.nlm.nih.gov/pmc/articles/PMC7309248/.
[95] eHealth Initiative, *Leveraging Patient Generated Health Data to Improve Outcomes and Decrease Cost*. Available at: www.ehidc.org/sites/default/files/resources/files/Leveraging%20Patient%20Generated%20Health%20Data%20to%20Improve%20Outcomes%20and%20Decrease%20Cost%20%28002%29.pdf.
[96] The Hill, *HIPAA Guidelines Should Evolve with Wearable Technology*, March 2018. Available at: thehill.com/opinion/healthcare/378450-hipaa-guidelines-should-evolve-with-wearable-technology?rl=1.
[97] Manatt, *A Shared Responsibility: Protecting Consumer Health Data Privacy in an Increasingly Connected World*, June 2020. Available at: www.ehidc.org/sites/default/files/resources/files/RWJFConsumerHealth.pdf.
[98] The California Consumer Privacy Act (CCPA) is a comprehensive privacy law that is not limited to one industry and applies to many technology companies. The law provides California residents with multiple rights regarding their data. The CCPA only applies to for-profit businesses operating in California; it does not apply to information that is subject to HIPAA. More information is available at: www.oag.ca.gov/privacy/ccpa.
[99] See n. 97, *Supra.*
[100] Medical Director, *Patient Generated Health Data and the Future of Wearable Technology*, September 2020. Available at: www.medicaldirector.com/news/future-of-health/2020/09/patient-generated-health-data-and-the-future-of-wearable-technology.
[101] Medical Group Management Association, *Most Practices Offer a Patient Portal,* July 2018. Available at: www.mgma.com/news-insights/quality-patient-experience/mgma-stat-most-practices-offer-a-patient-portal.
[102] The Patient Health Information Capture Criterion, §170.315(e)(3), states that a certified EHR must "enable a user to: 1) Identify, record, and access information directly and electronically shared by a patient (or authorized representative). 2) Reference and link to patient health information documents." More information is available at: www.healthit.gov/topic/otherhot-topics/what-are-pghd-related-criteria-health-it-rules-and-programs.
[103] The integration of PGHD into EHRs is in its infancy and may be underreported in available literature. Best practices on how to incorporate PGHD into clinical workflows are not yet available.
[104] Tiase VL, Hull W, McFarland MM, Sward KA, Del Fiol G, Staes C, Weir C, Cummins MR. Patient-Generated Health Data and Electronic Health Record Integration: A Scoping Review. JAMIA Open. Volume 3, Issue 4, December 2020, Pages 619–627. Available at: doi.org/10.1093/jamiaopen/ooaa052.
[105] For example, patient portals provide HIPAA compliant email where all communications happen within the confines of the software requiring a user to sign into the portal to retrieve and read emails.
[106] U.S. Department of Health & Human Services, *Your Rights Under HIPAA*, November 2020. Available at: www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html.
[107] See n. 97, *Supra.*
[108] HHS has clarified that PHI shared with a third-party application chosen by a patient is not covered by HIPAA.
[109] HealthTech, *3 Reasons Why Wearables Bring New Complications for HIPAA Compliance*, September 2020. Available at: healthtechmagazine.net/article/2020/09/3-reasons-why-wearables-bring-new-complications-hipaa-compliance.
[110] Minnesota Law Review, *Addressing the HIPAA-potamus Sized Gap in Wearable Technology Regulation*. Available at: minnesotalawreview.org/wp-content/uploads/2019/12/Papandrea_FINAL_MLR104-Updated.pdf.
[111] According to some (global) estimates, the health care-related Internet of Things (IoT) market, including sensor-enabled wearables, is projected to reach $534 billion by 2025, expanding at an annual rate of almost 20 percent. Another analysis predicts a 36 percent growth rate for health data over the next five years, a faster increase than in any other industry. More information is available at: www.ehidc.org/sites/default/files/resources/files/RWJFConsumerHealth.pdf.
[112] National Conference of State Legislatures, *Security Breach Notification Laws*, April 2021. Available at: www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
[113] Venable, *Newest Trends in Health Data Breaches: FTC, OCR, and AG Enforcement*, May 2021. Available at: www.venable.com/-/media/files/events/2021/05/newest-trends-in-health-data-breaches.pdf.
[114] Enacted as part of the American Recovery and Reinvestment Act of 2009. More information is available at: www.ftc.gov/system/files/documents/federal_register_notices/2009/08/healthbreachnotificationrulefinal.pdf.

[115] The Rule preempts contradictory state breach notification laws, but not those that impose additional – but non-contradictory – breach notification requirements (e.g., state laws that require breach notices to include advice on monitoring credit reports or contact information for consumer reporting agencies). More information is available at: www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule.
[116] FTC enforcement began on February 22, 2010.
[117] American Bar Association, *IoT Big Data: Consumer Wearables, Data Privacy, and Security,* December 2015. Available at: www.americanbar.org/groups/intellectual_property_law/publications/landslide/2015-16/november-december/IoT-Big-Data-Consumer-Wearables-Data-Privacy-Security/.
[118] See n. 97, *Supra.*
[119] ONC, *Conceptualizing a Data Infrastructure for the Capture, Use, and Sharing of Patient-Generated Health Data in Care Delivery and Research through 2024*, January 2018. Available at: hwww.healthit.gov/sites/default/files/onc_pghd_final_white_paper.pdf.
[120] Section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of protected health information. More information is available at: www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html.
[121] See, n. 117, *Supra.*
[122] See . 119, *Supra.*
[123] See n. 93, *Supra.*
[124] BMJ Journals, *Electronic Patient-Generated Health Data to Facilitate Prevention and Health Promotion: A Scoping Review Protocol,* August 2018. Available at: www.bmjopen.bmj.com/content/bmjopen/8/8/e021245.full.pdf.
[125] See n. 95, *Supra.*
[126] EPAM Insights, *Your Patients, Their Data: Why Patient-Generated Health Data Is Critical for the Future of Healthcare,* May 2020. Available at: www.epam.com/insights/blogs/patient-generated-heath-data-is-critical-for-the-future-of-healthcare.
[127] ONC and CMS published separate but related rules addressing interoperability, information blocking, standards to support data exchange, and patient access to electronic health information. The ONC rule implements interoperability provisions of the Cures Act to allow for seamless data exchange among providers, payers, and patients. The Final Rule was published on May 1, 2020 and went into effect on April 5, 2021. The CMS Rule includes policies that require payers to implement technology standards to improve electronic exchange of health information with patients, providers, and other payers. The Rule went into effect on January 1, 2021; however, CMS exercised enforcement discretion until July 1, 2021 due to the PHE. More information is available at: www.healthit.gov/curesrule/ and www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index.
[128] See n. 95, *Supra.*
[129] NEJM Catalyst, *What Is Patient-Centered Care*, January 2017. Available at: catalyst.nejm.org/doi/full/10.1056/CAT.17.0559.
[130] Patient Engagement HIT, *3 Benefits of Patient-Generated Health Data, Patient Engagement*, March 2016. Available at: patientengagementhit.com/news/3-benefits-of-patient-generated-health-data-patient-engagement.
[131] Experian, *How to Protect Your Privacy on Wearable Devices*, February 2018. Available at: www.experian.com/blogs/ask-experian/how-to-protect-your-privacy-on-wearable-devices/.
[132] See n. 97, *Supra.*
[133] See n. 93, *Supra.*
[134] Health IT Security, *Health Data Not Covered by HIPAA Needs Values Framework*, March 2019. Available at: healthitsecurity.com/news/health-data-not-covered-by-hipaa-needs-values-framework.
[135] *Ibid.*
[136] See n. 97, *Supra.*
[137] U.S. Department of Health & Human Services, *Summary of the HIPAA Security Rule,* July 2013. Available at: www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.
[138] HITECH amended previous federal legislation to strengthen privacy and security safeguards for electronic PHI, extending liability to BAs and their subcontractors. HITECH also established the Breach Notification Rule requiring CEs and BAs to provide prompt notification following a breach of unsecured PHI.
[139] Such practices must be in place for a minimum of 12 months prior to a breach.
[140] Health IT Security, *HIPAA Safe Harbor Bill Becomes Law; Requires HHS to Incentivize Security*, January 2021. Available at: healthitsecurity.com/news/hipaa-safe-harbor-bill-becomes-law-requires-hhs-to-incentivize-best-practice-security.
[141] U.S. Department of Health & Human Services Office of the Assistant Secretary for Preparedness and Response, *Legal Authority of the Secretary*, September 2019. Available at: www.phe.gov/Preparedness/support/secauthority/Pages/default.aspx.
[142] U.S. Department of Health & Human Services, *Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency,* January 2021. Available at: www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.
[143] Renal and Urology News, *Prepare for the End of Pandemic Telehealth Waivers*, November 2020. Available at: www.renalandurologynews.com/home/departments/hipaa-compliance/covid-19-pandemic-waiver-cybersecurity-hipaa/.
[144] The Secretary of Health & Human Services, *Public Health Message to Governors*, January 2021. Available at: ccf.georgetown.edu/wp-content/uploads/2021/01/Public-Health-Emergency-Message-to-Governors.pdf.

Center for Health Information Technology and Innovative Care Delivery

4160 Patterson Avenue

Baltimore, MD 21215

410-764-3460

www.mhcc.maryland.gov