American Journal of Emergency Medicine xxx (xxxx) xxx

Contents lists available at ScienceDirect

American Journal of Emergency Medicine

journal homepage: www.elsevier.com/locate/ajem

Cyberthreats: A primer for healthcare professionals

Derrick Tin, MBBS [a,1,*], Ryan Hata, MD [a,1], Fredrik Granholm, MD [b], Robert G. Ciottone, BA [a], Richard Staynings [c], Gregory R. Ciottone, MD [a]

[a] Disaster Medicine Division, Department of Emergency Medicine, Beth Israel Deaconess Medical Center and Harvard Medical School, United States
[b] Swedish Air Ambulance (SLA), Mora, Sweden
[c] University of Denver, University College, United States

ARTICLE INFO

Article history:
Received 17 February 2023
Received in revised form 23 March 2023
Accepted 1 April 2023
Available online xxxx

ABSTRACT

Introduction: Cyberattacks are one of the most widespread, damaging, and disruptive forms of action against healthcare entities. Data breaches, ransomware attacks, and other intrusions can lead to significant cost both in monetary and personal harm to those affected and may result in large payouts to cyber criminals, crashes of information technology systems, leaks of protected health and personal information, as well as fines and lawsuits. This study is a descriptive analysis of healthcare-related cyber breaches affecting 500 or more individuals in the past decade in the United States.

Methods: The publicly available U.S. breach report database was downloaded in the Microsoft Excel (Microsoft, Redmond, Washington, USA) format and searched for all reported breaches occurring between January 1, 2011 - December 31, 2021 (10 years). Breaches were subdivided by category and analyzed by states, breach submission dates, types of breach, location of breached information, entity type, and individuals affected. All subcategories were predefined by the breach report.

Results: There were a total of 3822 PHI breaches that affected 283,335,803 people in the United States from January 1, 2011 to December 31, 2021. Of the 3822 PHI breaches, 1593 (41.7%) were hacking/ IT related, 1055 (27.6%) were listed as unknown, 819 (21.4%) were theft related, 194 (5.1%) were loss related, 97 (2.5%) were related to improper disposal and 64 (1.7%) were listed as "others". Year 2020 saw the most breaches with 631 and California was the state with the highest number of breaches at 403.

Conclusion: Cyberattacks and healthcare breaches are one of the most costly and disruptive situations facing healthcare today. A total of 3822 breaches affecting 283,335,803 people in the United States were recorded from January 1, 2011 to December 31, 2021. By understanding the extent of cyberthreats this will better prepare healthcare organizations and providers to mitigate, respond, and recover from these devastating attacks.

1. Introduction

Cyberattacks against healthcare have been growing at an alarming rate globally as cybercriminals and pariah nation-states target the industry for its treasure trove of non-public information [1]. This includes the theft of clinical research intellectual property (IP), personally identifiable information (PII), and personal health information (PHI). The healthcare sector experiences twice as many cyberattacks as other industries with the United States bearing the brunt of most of these health-related attacks over the past decade [2,3].

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was put in place to protect the confidentiality, integrity, and availability of PHI from exposure to unauthorized persons or entities (otherwise known as a "breach," though exemptions do apply in certain circumstances). HIPAA is a mandatory law in the USA for covered entities and non-compliance can result in significant fines of up to 1.5 million USD per year [4].

The Health Information Technology for Economic and Clinical Health (HITECH) Act expands the HIPAA encryption compliance requirement set, requiring the disclosure of data breaches of unencrypted personal health records by healthcare providers, health plans, healthcare clearinghouses, as well as related entities such as business associates and

Abbreviations: CEs, Covered Entities; HITECH, Health Information Technology for Economic and Clinical Health; HIPAA, The Health Insurance Portability and Accountability Act of 1996; IoT, Internet of Things; IT, Information Technology; PHI, Personal Health Information; PII, Personally Identifiable Information.

* Corresponding author.
E-mail addresses: dtin@bidmc.harvard.edu (D. Tin), rhata1@bidmc.harvard.edu (R. Hata), fredrik.granholm@regiondalarna.se (F. Granholm), rciotton@bidmc.harvard.edu (R.G. Ciottone), richard.staynings@du.edu (R. Staynings), gciotton@bidmc.harvard.edu (G.R. Ciottone).
[1] Joint First Co-Author.

https://doi.org/10.1016/j.ajem.2023.04.001
0735-6757/

Table 1
Breach breakdown by covered entities.

Covered Entity type	Number of breaches	Number individuals affected
Health Care Provider	2981 (74.0%)	112,183,693 (37.0%)
Health Plan	518 (12.9%)	122,971,520 (40.5%)
Business Associate	513 (12.7%)	66,451,137 (21.9%)
Health Care Clearing House	10 (0.02%)	1,648,824 (0.5%)
Other	4 (0.01%)	29,626 (0.01%)
Total	4026	303,284,800

vendors [5]. Collectively, these organizations and individuals are termed "covered entities" (CEs) and have either direct or indirect access to, store, transmit, or use PHI on a regular basis.

This paper is a descriptive analysis of PHI and healthcare-related cyber breaches affecting 500 or more individuals in the past decade in the United States. This may help healthcare providers understand the extent of the issue and mitigate some of the associated risks.

2. Methods

As required by section 13402(e)(4) of the HITECH Act, the Secretary of the Department of Health and Human Resources must post a list of breaches of unsecured protected health information affecting 500 or more individuals [6]. A breach is defined as an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information, and the breach report database is publicly accessible through the United States (U.S.) Department of Health and Human Services Office for Civil Rights portal [7].

The publicly available U.S. breach report database was downloaded in the Microsoft Excel (Microsoft, Redmond, Washington, USA) format and searched for all reported breaches occurring between January 1, 2011 - December 31, 2021 (10 years). Breaches were subdivided by category and analyzed by states, breach submission dates, types of breach, location of breached information, entity type, and individuals affected. All subcategories were predefined by the breach report.

3. Results

There were a total of 4026 PHI breaches that affected 303,284,800 people in the United States from January 1, 2011 to December 31, 2021. The most reported breach events were directed toward healthcare providers with 2981 (74%) breaches affecting 112,183,693 (37%) individuals, followed by health plans (518 [13%]) affecting 122,971,520 (41%) individuals, business associates (513 [13%]) affecting 66,451,137 (22%) individuals, and healthcare clearing houses (10 [0.2%]) affecting 1,648,824 (0.5%) individuals. Four (0.1%) breaches were from other sources and affected 29,626 (0.01%) individuals. (Table 1 and Figs. 1 and 2). (See Table 2.)

Types of breaches were broken down into seven primary categories, with several subcategories for each type. The seven major categories were: hacking/IT incidents, unauthorized access/disclosure, theft, loss, improper disposal, other, and unknown.

Of the 4026 PHI breaches, 1742 (43%) were primarily hacking/ IT related, 1087 (27%) were primarily related to unauthorized access or disclosure, 828 (21%) were primarily theft related, 197 (5%) were primarily loss related, 98 (2%) were primarily due to improper disposal, 64 (1.5%) were other, and 10 (0.2%) were unknown.

Year 2020 saw the most breaches with 661. This was followed by 2021 (519), 2019 (512), 2018 (369), 2017 (358), 2016 (329), 2014 (314), 2013 (276), 2015 (270), 2012 (218), and 2011 (200). 2020 also had the most individuals affected at 111,697,151. 2011 saw the lowest number of data breaches (200), and also had the lowest number of people affected at 5,963,172 (Table 3 and Figs. 3 and 4).

States were analyzed for number of breaches and number of individuals affected. California was the state with the highest number of breaches at 424 with 17,539,817 individuals affected. This was followed by Texas (333 breaches, 10,810,863 affected), Florida (259 breaches, 21,224,605 affected), New York (227 breaches, 22,110,054 affected),

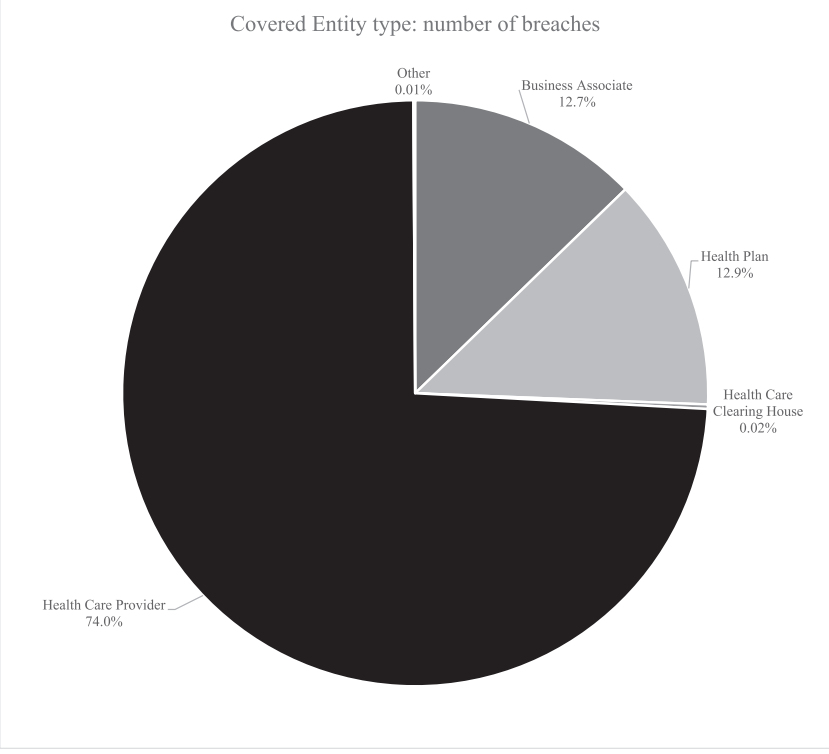

Fig. 1. Covered Entity type: number of breaches.

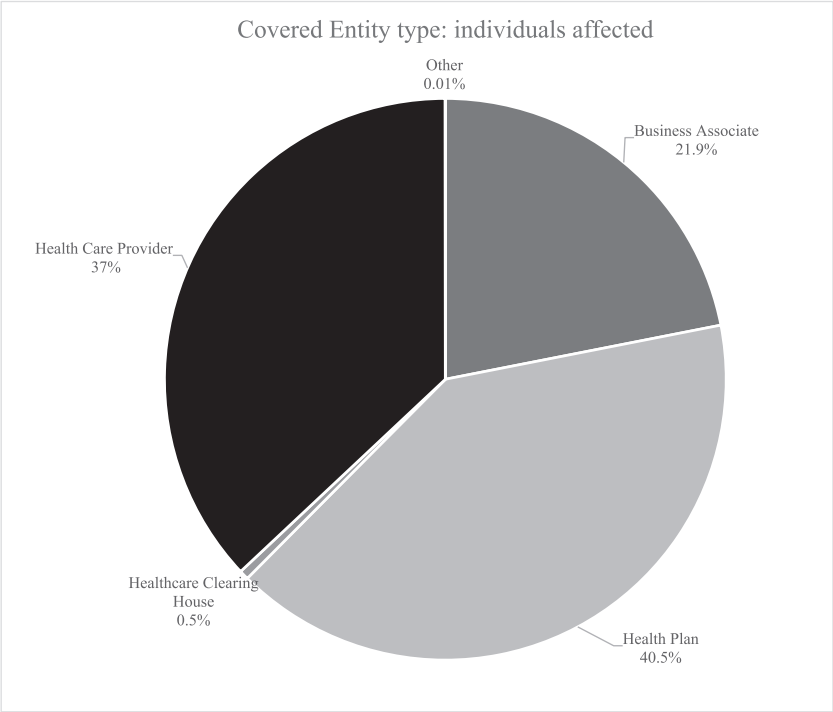

Fig. 2. Covered Entity type: individuals affected.

and Illinois (170 breaches, 6,452,987 affectEd.) Despite California having the highest number of breaches, the total number of people affected was lower than both Florida and New York.

The states with the lowest total number of breaches were Idaho with 8 breaches affecting 173,927 individuals, followed by South Dakota (9 breaches, 39,038 affected,) North Dakota (9 breaches, 56,377 affected,) Vermont (10 breaches, 103,899 affected,) other U.S. territories (10 breaches, 2,939,639 affected,) and Wyoming (12 breaches, 80,993 affectEd.) (Table 4.)

Location of breached information was divided into seven main categories: desktop computer, electronic medical record, email, laptop computer, network server, other, and paper/film. Network servers had the highest number of breaches at 1043 (26%) and affected 227,686,822 individuals, followed by email (965 [24%], 30,071,008 affected,) paper/film (677 [17%], 5,315,442 affected,) other (460 [11%], 15,758,977 affected,) laptop (344 [9%], 5,662,706 affected,) desktop computer (308 [8%], 11,529,003 affected,) and electronic medical records (229 [6%], 7,260,842 affectEd.) (Table 5.)

4. Discussion

Healthcare/Public Health represents one of the sixteen critical infrastructure sectors considered vital to the United States [8]. With over 303 million people in the U.S. affected by cyberbreaches in the past ten years, these attacks have become one of the paramount concerns of providers, healthcare systems, and the state and federal government. According to International Business Machines Corporation's (IBM) Cost of a Data Breach Report 2022, healthcare had the highest breach-related financial damages of all industries for 12 consecutive years, with cyberattacks costing an average of $10.1 million per breach, up 9.4% from one year earlier [9].

A data breach may be caused by malicious action, human error, or a failure in information handling or security systems, and can cause significant harm in multiple ways, including serious physical or psychological harm, financial loss, identity theft, and reputational damage [10]. There have also been instances of significant safety and security concerns for victims (particularly victims of domestic abuse) after a data breach, leading to intimidation, embarrassment, and humiliation, as well as family violence [11]. Recent studies have also shown a concerning correlation between cyberattacks and patient morbidity and mortality rates [12].

Medical data, in particular, is an especially attractive proposition for malicious actors. Whereas credit card information and Social Security numbers can be sold on the dark web for $1- $15, personal medical

Table 2
Breach breakdown by type.

Type of breach	Number of breaches
Hacking/IT incident	1742 (43%)
Unauthorized Access/Disclosure	1087 (27%)
Theft	828 (21%)
Loss	197 (5%)
Improper disposal	98 (2%)
Other	64 (1.5%)
Unknown	10 (0.2%)
Total	**4026**

Table 3
Breaches by breach submission dates.

Year	Number of data breaches	Number of individuals affected
2021	519	32,916,817
2020	661	34,575,557
2019	512	44,964,471
2018	369	14,232,822
2017	358	5,306,786
2016	329	16,712,554
2015	270	112,466,720
2014	314	19,073,551
2013	276	7,018,839
2012	218	2,854,525
2011	200	13,162,158
Total	**4026**	**303,284,800**

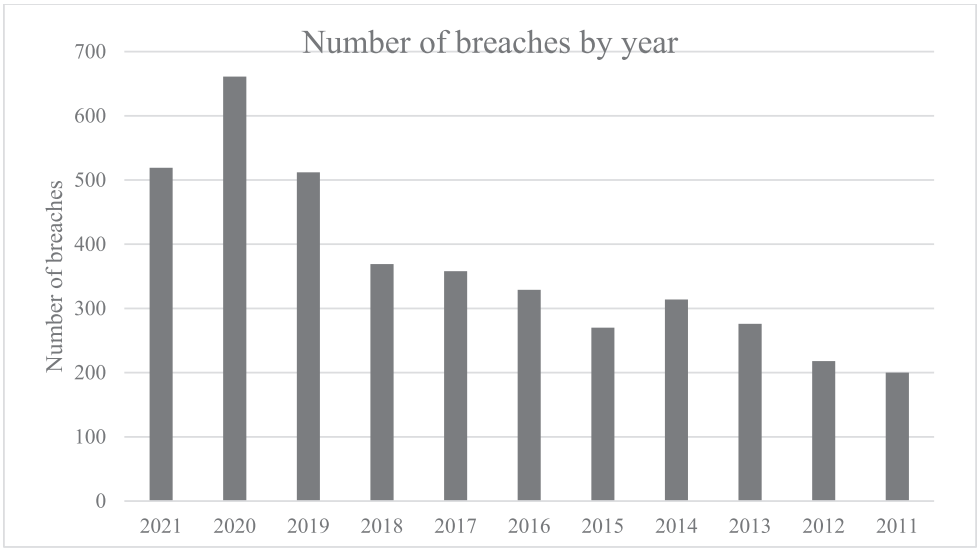

Fig. 3. Number of breaches by year.

data can sell for around $60 [13]. It is estimated that the per-record cost of a data breach in 2022 was $164, a 12.3% increase from 2020 [14].

Financial gains aside, healthcare companies have increasingly been targets of foreign government cyberattacks with nefarious political and disruptive motives, and many security experts today consider cyberattacks a top national security concern [15].

5. Trends

Malicious breaches, whether specifically targeted or broad in nature, have been rising sharply. It is a well-documented that Russia, in particular, has recently been using cyberattacks to target critical infrastructure with strategies such as distributed denial of service (DDoS) attacks and deployment of malicious malware [16]. Breaches in the first five months of 2022 having doubled over the prior year [17]. While the number of annual data breaches has trended up several years in a row, 2020 showed a significant increase in data breaches, likely due to multiple factor including an increase in cybersecurity attacks on healthcare organizations due to the COVID-19 pandemic [18].

Despite an increase in the overall number of cyberbreaches affecting CE's, the total number of individuals affected does not necessarily correlate with the number of breaches. The sharp spike in individuals affected in 2015, for example, was primarily due to a single data breach affecting nearly 79 million individuals. This breach was one of the largest in history and cost the CE, Anthem Incorporated insurance company, nearly $16 million in fines to the Department of Health and Human Service and an additional $39.5 million in settlements to U.S. States Attorneys General [19,20].

It is important to state that not all cyberattacks against healthcare CEs result in a breach of PHI. Often the perpetrators are after intellectual property (IP) data such as clinical research and drug trial data. Many US and EU hospitals were hit in early 2020 with cyberattacks of this nature, mostly from Russia, North Korea, China, and Iran, as the world searched for an effective vaccine to COVID-19 [21,22]. One such attack even prompted warnings of retaliatory consequences from US Secretary of

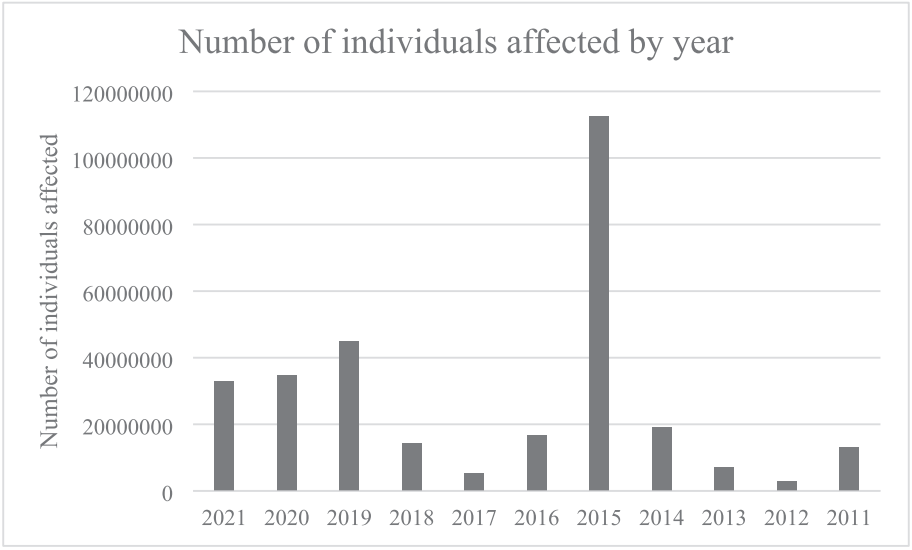

Fig. 4. Number of individuals affected by year.

Table 4
Number of breaches and individuals affected by states.

State/Territory	Number of Breaches	Number of individuals affected
AK	17	594,561
AL	44	1,664,923
AR	55	781,629
AZ	92	7,724,363
CA	424	17,539,817
CO	77	1,119,029
CT	73	1,915,604
DC	14	449,606
DE	17	495,554
FL	259	21,224,605
GA	119	471,0013
HI	13	247,150
IA	57	1,926,515
ID	8	173,927
IL	170	6,452,987
IN	107	85,430,834
KS	27	361,851
KY	76	1,632,793
LA	39	738,504
MA	108	1,780,658
MD	89	5,430,451
ME	15	405,407
MI	112	4,800,771
MN	109	13,088,053
MO	93	2,409,738
MS	26	240,050
MT	20	135,2827
NC	95	1,437,2451
ND	9	56,377
NE	31	570,698
NH	14	341,657
NJ	73	4,223,887
NM	36	3,009,723
NV	33	475,913
NY	227	22,110,054
OH	139	6,385,345
OK	34	1,890,407
OR	67	2,015,032
PA	165	3,868,746
PR	26	721,315
RI	20	131,572
SC	45	1,524,160
SD	9	39,038
TN	90	13,078,176
TX	333	10,810,863
UT	34	1,667,365
VA	74	10,346,752
VT	10	103,899
WA	97	14,507,196
WI	58	3,197,807
WV	25	123,515
WY	12	80,993
Other Territories	10	2,939,639
Total	**4026**	**303,284,800**

State Mike Pompeo [23]. Ransomware has also been a significant attack modality for healthcare-related breaches. Today, healthcare experiences twice the number of cyberattacks as other industries [24].

6. Attack surfaces: exploiting system vulnerabilities

The healthcare industry worldwide has undergone a massive digital transformation over the past decade. No country has changed more quickly or deeply than the United States, which has been led by government initiatives and monetary incentives to drive the adoption of digital patient records and interoperability to support "meaningful use." [25,26] With this increase digitalization come not only increases in efficiency and financial incentives, but also an increased attack surface that puts many healthcare providers at risk for data breaches. Indeed, healthcare providers make up 74% of breaches, with 43% of breaches resulting from hacking or information technology (IT) compromise. Network servers and email are particularly vulnerable, making up 50% of the attack surfaces.

Table 5
Breaches by location.

Location of breach	Number of breaches	Number of individuals affected
Network Server	1043 (26%)	227,686,822
Email	965 (24%)	30,071,008
Paper/film	677 (17%)	5,315,442
Other	460 (11%)	15,758,977
Laptop	344 (9%)	5,662,706
Desktop Computer	308 (8%)	11,529,003
Electronic Medical Record	229 (6%)	7,260,842
Total	**4026**	**3,032,848,000**

The recent and ongoing expansion of medical and other healthcare "internet of things" (IoT) devices, together with the growing number of connected hospital building management systems, has further expanded the attack surface. A 2019 report claimed that almost 50% of endpoints on hospital networks are unmanaged devices [27]. While some of this may be attributable to "bring your own device" (BYOD) and guest devices, a large part is attributable to growing levels of medical and other healthcare IoT [28].

Some medical devices are very expensive to procure and so are amortized on health system books over a lengthy period. Other devices are inexpensive and seemingly innocuous yet continue to work well for many decades of service. Few medical devices, however, are patched [29]. Indeed, security support for these devices by manufacturers is poor at best, as are timely release of patches to critical security vulnerabilities (CVEs) [30]. Most devices were never designed for the future and so lack the capacity to run upgraded software. Given an average lifespan of 10 to 15 years and a design that for most did not really consider today's cybersecurity environment, many are now highly vulnerable to attack, and unless mitigated can pose a risk to the entire medical network [31].

7. Imbalance

With 337 healthcare breaches reported in the first 6 months of 2022 there is a 75.6% chance of a breach of at least five million records in the next year [32,33]. Healthcare cybersecurity teams have to protect every system, every byte of data, and every mile of their networks, every hour of every day. Perpetrators on the other hand only need to find one small weakness or exploit a single vulnerability to gain a foothold from which to expand their presence. Just as the odds are stacked against defenders, so too is the resource imbalance. Cybercriminals often have significant resources at their disposal, and may be state-sponsored actors. In addition, cybercriminal organizations may reside outside the jurisdiction of the country where the crime takes place, thus making extradition complicated at best and nearly impossible at worst [34]. Due to this imbalance it is imperative that governments and law enforcement agencies use every tool at their disposal to secure healthcare system cybernetworks and bring criminals to justice.

8. Emergency departments

Emergency departments are often considered the gatekeepers of health systems around the world. A breach in cyber security could potentially immediately affect critically unwell patients as well as have downstream consequences within hospitals [35]. The authors advocate for better understanding of cyberthreats for ED staff and better preparedness and mitigation, strategies such as regular risk assessments to identify vulnerabilities (IT system, networks, devices), development

and simulation of cyber-incidence response strategies, and regular education for staff to better identify threats such as phishing emails and malware infections. In the event of a cyberbreach, emergency physicians must be prepared to lead in the response efforts by effectively using downtime procedures and protocols to minimize departmental and patient impacts. In the recovery phase after a cyberattack, emergency physicians should be integral in identifying areas of improvement and implementing new strategies to maintain continuity of care, as well as collaborating with hospital administrators, IT professionals, and law enforcement officials to prevent further attacks.

So, in a land of near-constant change, what do stakeholders need to know to protect their patients and organizations? While special interest programs such as Disaster Medicine and Counter-Terrorism Medicine discuss the impact of cyberthreats on healthcare systems [36], cybersecurity training within the healthcare sector remains woefully lacking, and health systems unprepared. With a threat surface that changes almost daily and highly creative and adaptive adversaries, ongoing effective cybersecurity training should be a necessary requirement for all who work in this industry. In the same spirit of constant innovation and discovery that healthcare utilizes to combat illness and injury, so must it address in an equally proactive way the evolving cyberthreat landscape. The solution lies in bridging the valley between healthcare advances and cybersecurity advances, and it is dependent on stakeholders in both, as well as society as a whole, to span that potentially catastrophic chasm.

9. Limitations

This study was limited to breaches affecting 500 people or more only, as reported by the entities. While the U.S. Department of Health and Human Services' breach database is the most comprehensive database of its kind, breaches affecting 500 or fewer people were not available. It is unknown exactly what percentage of healthcare breaches in the United States go unreported, but we can look to other jurisdictions such as Europe, where it has been reported that over 75% of data breaches go unreported [37]. While entities have breach notification obligations and The.

Office for Civil Rights (OCR) is able to impose substantial civil penalties for organizations that fail to comply, if there are incidents not reported, this could limit the accuracy of the findings [6].

Using pre-existing databases as a data source also inherently introduces potential challenges. Miscoding errors, data entry errors, or missed data may all occur, limiting the validity of the database.

10. Conclusion

A total of 4026 breaches affecting 303,284,800 people in the United States were recorded from January 1, 2011 to December 31, 2021. The most reported breaches were from healthcare providers with 2981 (74%) of events, followed by health plans (518 [13%]), business associates (513 [13%]) and healthcare clearing houses (10 [0.2%]). 4 (0.1%) breaches were from unknown sources. This report may help healthcare providers understand the extent of the issue and mitigate some of the associated risks and highlights the challenges the healthcare industry faces in protecting patient data in an era of escalating cyberthreats.

CRediT authorship contribution statement

Derrick Tin: Writing – original draft, Data curation, Conceptualization. **Ryan Hata:** Writing – review & editing, Writing – original draft. **Fredrik Granholm:** Writing – review & editing. **Robert G. Ciottone:** Data curation. **Richard Staynings:** Writing – review & editing. **Gregory R. Ciottone:** Writing – review & editing, Supervision.

Declaration of Competing Interest

The authors have no financial disclosures and no conflicts of interest.

"This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors".

DT and RH participated in the conception and design of the research. DT and RH acquired and analyzed the data. DT, RH and RS contributed to writing the manuscript. FG, RC and GC reviewed the results and overall manuscript. All authors have read the manuscript and approved its submission.

References

[1] Paul K. Lives are at stake: hacking of US hospitals highlights deadly risk of ransomware. *The Guardian*; 2022. https://www.theguardian.com/technology/2022/jul/14/ransomware-attacks-cybersecurity-targeting-us-hospitals Published 2022. Accessed November 4, 2022.

[2] Healthcare Experiences Twice the Number of Cyber Attacks As Other Industries. CSO Online; 2023. Accessed March 22, 2023. https://www.csoonline.com/article/3260191/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html.

[3] Health Sector Cybersecurity. 2021 Retrospective and 2022 look ahead. HHS Cybersecurity Program; 2022 Published online 2022.

[4] HIPAA Breach Notification - What you need to know. Tripwire Published 2020. Accessed November 4, 2022. https://www.tripwire.com/state-of-security/hipaa-breach-notification-what-need-know; 2022.

[5] What is HIPAA and HITECH Compliance? Thales. Accessed November 4, 2022. https://cpl.thalesgroup.com/faq/americas-compliance/what-hipaa-hitech; 2022.

[6] Chapter 7: Breach Notification, HIPAA Enforcement, and Other Laws and Requirements. *The Office of the National Coordinator for Health Information Technology: Guide to Privacy and Security of Electronic Health Information*; 2022; 56–62.

[7] U.S. Department of Health & Human Services - Office for Civil Rights. Accessed March 22, 2023. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf; 2023.

[8] Critical infrastructure sectors. Critical infrastructure sectors. Published 2022. Accessed November 4, 2022. https://www.cisa.gov/critical-infrastructure-sectors.

[9] Cost of a dData Breach. IBM Corporation Published 2022. Accessed November 4, 2022. https://www.ibm.com/reports/data-breach; 2022.

[10] Part 1: Data breaches and the Australian Privacy Act.. Office of the Australian Information Commissioner; 2022. Published 2019. Accessed November 4, 2022. https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-1-data-breaches-and-the-australian-privacy-act.

[11] Managing the Privacy Impacts of a Data Breach. Office of the Victorian Information Commissioner; 2022. Published 2019. Accessed November 4, 2022. https://ovic.vic.gov.au/privacy/resources-for-organisations/managing-the-privacy-impacts-of-a-data-breach/.

[12] Study confirms increase in mortality rate and poorer patient outcomes after cyberattacks. hipaajournal.com Published 2022. Accessed November 4, 2022. https://www.hipaajournal.com/study-confirms-increase-in-mortality-rate-and-poorer-patient-outcomes-after-cyberattacks/; 2022.

[13] Morrissey D. Malicious actors and medical data: where are we heading? AT&T Cybersecurity. Published 2020. Accessed November 4, 2022. https://cybersecurity.att.com/blogs/security-essentials/malicious-actors-and-medical-data-where-are-we-heading.

[14] Cyber Insecurity In Healthcare: The Cost And Impact On Patient Safety And Care, Ponemon Institute Report 2022.

[15] Dreyfuss E. As cyberattacks destabilize the world, the State Department turns a blind eye. Wired. Published 2022. Accessed November 4, 2022. https://www.wired.com/story/state-department-cybersecurity/.

[16] Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. CISA; 2022. Accessed December 2, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.

[17] Peyton D. Healthcare breaches on the rise in 2022. techtarget.com Published 2022. Accessed November 4, 2022. https://www.techtarget.com/searchsecurity/news/252521771/Healthcare-breaches-on-the-rise; 2022.

[18] Ignatovski M. Healthcare breaches during COVID-19: the effect of the healthcare entity type on the number of impacted individuals. Perspect Health Inf Manag. 2022.; 19(4).

[19] Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History | Guidance Portal. Accessed March 21, 2023. https://www.hhs.gov/guidance/document/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-us-health-data-breach.

[20] Anthem to pay nearly $40 million to settle data breach probe by U.S. states | Reuters. Accessed March 21, 2023. https://www.reuters.com/article/us-anthem-cyber/anthem-to-pay-nearly-40-million-to-settle-data-breach-probe-by-u-s-states-idUSKBN26L2PW.

[21] Cimpanu C. Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak. ZDnet; 2022. Published 2020. Accessed November 4, 2022. https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/.

[22] Blankenship K. China, Iran hackers fingered for targeting COVID-19 vaccine R&D: reports | FiercePharma. fiercepharma.com Published 2020. Accessed November 4,

2022. https://www.fiercepharma.com/pharma/gilead-target-iranian-cyberattack-for-role-covid-19-response-report; 2022.
[23] Pamuk H, Brice M, Hepinstall S. U.S. Says concerned by threat of cyber attack against Czech Republic healthcare - Reuters. Reuters; 2022. Published 2020. Accessed November 4, 2022. https://www.reuters.com/article/us-czech-cyber-usa/u-s-says-concerned-by-threat-of-cyber-attack-against-czech-republic-healthcare-idUSKBN22000J.
[24] Healthcare Experiences Twice the Number of Cyber Attacks As Other Industries | CSO Online. Accessed November 4, 2022. https://www.csoonline.com/article/3260191/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html.
[25] Promoting Interoperability Programs | CMS. Accessed November 4, 2022. https://www.cms.gov/regulations-and-guidance/legislation/ehrincentiveprograms.
[26] Anumula N, Sanelli PC. Meaningful use. AJNR Am J Neuroradiol. 2012;33(8):1455. https://doi.org/10.3174/AJNR.A3247.
[27] What Makes IoMT Devices So Difficult to Secure Against Cyberthreats. Accessed November 15, 2022. https://healthtechmagazine.net/article/2020/02/what-makes-iomt-devices-so-difficult-secure-perfcon.
[28] Report: 72% Orgs Faced Increase in IoT, Endpoint Security Incidents. Accessed November 15, 2022. https://healthitsecurity.com/news/report-72-orgs-faced-increase-in-iot-endpoint-security-incidents.
[29] Brooks R, Branch J. Your Medical Device Software Will Need Updated — Better Plan For It Now. MedDeviceOnline.com. Accessed November 4, 2022. https://www.meddeviceonline.com/doc/your-medical-device-software-will-need-updated-better-plan-for-it-now-0001.
[30] Miliard M. PATCH act seeks to shore up security for medical devices, IoT networks. Healthcare IT News; 2022. Published 2022. Accessed November 4, 2022. https://www.healthcareitnews.com/news/patch-act-seeks-shore-security-medical-devices-iot-networks.
[31] Staynings R. Understanding medical device security. Published online 2019. Accessed November 4, 2022. https://www.cyberthoughts.org/2017/09/understanding-medical-device-security.html; 2022.
[32] McKeon J. Health sector suffered 337 healthcare data breaches in first half of year. HealthITSecurity.com Published 2022. Accessed November 4, 2022. https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.
[33] Georgiev D. 25+ alarming healthcare data breaches statistics 2022. TechJuryNet Published 2022. Accessed November 4, 2022. https://techjury.net/blog/healthcare-data-breaches-statistics/.
[34] Why hackers are attacking healthcare more frequently?. Security Magazine; 2022. Accessed March 22, 2023. https://www.securitymagazine.com/articles/98860-why-hackers-are-attacking-healthcare-more-frequently.
[35] Dameff C, Farah J, Killeen J, Chan T. Cyber disaster medicine: a new frontier for emergency medicine. Ann Emerg Med. 2020;75(5):642–7. https://doi.org/10.1016/j.annemergmed.2019.11.011.
[36] Counter-Terrorism Medicine. Disaster Medicine Fellowship | BIDMC | Harvard Medical Faculty Physicians. Accessed November 16, 2022. https://www.disasterfellowship.org/counter-terrorism-medicine.
[37] Campbell N. Over 75% of data breaches unreported. Cleaver Fulton Rankin; 2022. Published 2019. Accessed November 4, 2022. https://cleaverfultonrankin.co.uk/legal-update/over-75-of-data-breaches-unreported/.