PROTENUS®

Copyright © 2024 Protenus | All Rights Reserved.

2024 Breach Barometer®

A look back at 2023 and insight on what 2024 could hold for healthcare data breaches

Health systems overwhelmed with unprecedented
171M patient records breached in 2023

PROTENUS®

In collaboration with DataBreaches.net

Contents

Introduction

When it comes to healthcare data breaches, 2023 was a year of unprecedented numbers and significant consequences. In this report, we will delve into the details of what made 2023 such a challenging year for healthcare organizations, their business associates and their patients. We will also explore potential trends and threats for 2024.

As you'll read in this report, 2023 breaches were monopolized by hackers. And while hackers remain the biggest cause or source of health data breaches, insider threats continue to impact organizations' ability to control from within. With technological gaps, continued disruption with mergers and acquisitions, healthcare resource constraints, and inconsistent risk assessment and analysis, healthcare organizations and their patient data remain vulnerable - making it easy for threat actors to find new and different ways to gain access.

In November 2023, New York Governor Kathy Hochul announced the **release** of "nation-leading statewide proposed cybersecurity regulations for hospitals, which will help the state's hospitals establish policies and procedures to safeguard health care systems from growing cyber threats." The proposed regulations aim to strengthen the protections on hospital networks and systems that are critical to providing patient care, as a complement to the HIPAA Security Rule that focuses on protecting patient data and health records. Under the proposed provisions, hospitals will be "required to establish a cybersecurity program and take proven steps to assess internal and external cybersecurity risks, use defensive techniques and infrastructure, implement measures to protect their information systems from unauthorized access or other malicious acts, and take actions to prevent cybersecurity events before they happen." Could this perhaps become a trend other states will adopt to help secure their systems and safeguard patient health data? Meanwhile, the OCR continues to ramp up enforcement efforts with an increase of budgetary spending and several significant monetary penalties.

While the data continually shows that breaches are on the rise, it is still likely that the volume and impact of healthcare data breaches continue to be underreported overall and underrepresented to the public. This retrospective report examines the extent of known health data breaches in 2023, going beyond those that are reported to the government, to provide the most complete picture possible – though gaps in detection and reporting mean the true impact of incidents is likely even greater. By aggregating all available data and analyzing the data from all perspectives, this report aims to arm healthcare and business leaders with the best understanding of the data breach landscape in healthcare. [Readers should refer to the Methodology section at the end of this report for detailed information on how data was coded and compiled.]

And finally, our report also explores preventative actions in the hopes of enabling healthcare organizations to take more effective, proactive postures going forward to eliminate risk.

Overview of 2023 Findings

A staggering 171 million patient records were breached in 2023. This number includes both breaches reported to HHS under HIPAA and incidents involving health data not covered by HIPAA but held by U.S. entities. A further breakdown of the data shows that in 2023, there were 1,161 reports published on both covered and non-covered entities (Figure 1), impacting a total of 171,139,241 breached records (Figure 2). For comparison, in 2022 there were 1,138 reports affecting a total of 59,664,152 breached records.

Figure 1.
Number of Breaches Reported

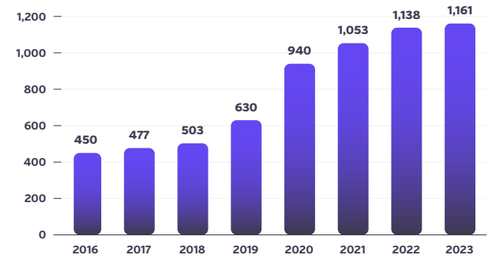
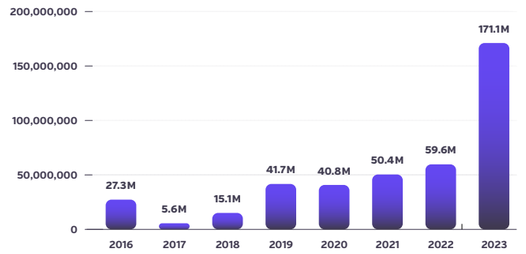


Figure 2.
Number of Records Breached



As in past years, we believe our 2023 numbers are significant underestimates because:

- We have no information into the number of patients affected for 200 of the reported incidents, and
- We have incomplete information for many other incidents, including 53 incidents that used "markers" to report incidents.

Figure 2 depicts the number of breached records reported by the Breach Barometer each year from 2016-2023. Although not represented in Figure 2, the staggering 171M figure can only be compared to the 2015 data reported by HHS of more than 110 million records breached, which in large part was due to one single breach involving Anthem Inc. that impacted more than 79 million individuals.

Year over year, the number of breaches reported increased 2% in 2023: while the number of actual incidents dropped 1%, to 942 in 2023, compared to 956 in 2022 and 905 in 2021. However, the number of patient records affected in 2023 was up 187% over 2022, when a total of 171,139,241 patient records were compromised (320% over 2020) in 942 incidents where this measure of breach impact was known. It is important to note that the total volume of patients impacted cannot be known until investigations have been completed, and the true number is undoubtedly higher.

The number of patient records affected in 2023 was up 187% over 2022

In 2023, we recorded 53 instances where entities submitted "500" or "501" as markers to indicate that they knew more than 500 patients or members were affected but did not yet have the total number. As readers will learn in the results portion of this report, the vast majority of markers never got updated by the end of 2023. Databreaches.net has informed us of their numerous attempts to reach out to HHS for more information on these placeholder instances. HHS has not responded as of the date of this report.

© Protenus 2024 | All Rights Reserved

Top Health Breaches of 2023

The largest contributors to data breaches in 2023 were due to software vulnerabilities found in file transfer solutions and exploited by the criminal ransomware organization Cl0p. Such breaches may be reported independent of those reported to HHS, as outlined in the section titled "Who Reports Breaches" later in this report. Therefore, Table 1 represents the top health breaches reported to HHS, using its public reporting tool.

The MOVEit breach affected 2,620 organizations (not all healthcare) that either used the software on their own platform or who used vendors who used the MOVEit software. Over 130 organizations (not all healthcare) reported ransomware attacks associated when GoAnywhere software was exploited. If one were to combine all the reports that involved these exploits, we might easily find that both software exploits were overwhelmingly the largest incidents of the year. When we see business associates who reported on behalf of clients for the MOVEit breach, the GoAnywhere breach, or other incidents, the numbers (such as those documented for Welltok) are only for their clients who had them do the reporting on their behalf. There may be – and likely are – other clients that were also affected by these same vulnerabilities who chose to do their own reporting to HHS. Because HHS does not require business associates to disclose the total number of patients affected across all of their clients in just one report, we do not have total numbers for many business associates.

Organization	Organization Type that Caused Breach	Number of Records Affected
HCA Healthcare	Provider / Business Associate	**11,270,000**
Perry Johnson & Associates	Business Associate	**8,952,212** plus an additional 3,998,162 with Concentra report
Managed Care of North America (MCNA)	Business Associate	**8,861,076**
Welltok	Business Associate	**8,493,379**
PharMerica Corporation	Provider	**5,815,591**
HealthEC	Business Associate	**4,452,782**
Reventics	Business Associate	**4,212,823**
Colorado Dept. of Health Care Policy & Financing	Health Plan	**4,091,794**
Regal Medical Group, Lakeside Medical Organization, ADOC Acquisition & Greater Covina Medical	Provider	**3,388,856**
CareSource	Business Associate	**3,180,537**

Table 1. Largest new incidents by month, 2023 health data breaches

Largest Single New Incidents by Month

Table 2 (shown on the next page) reports the largest single new incidents by month. In 2023, reporting of a breach was not necessarily reported by the organization that experienced the breach. For example, if the media reported on a covered entity breach, the name was entered and coded as a provider even though they had not actually made the disclosure or report.

Month	Organization	Organization Type	# of Breached Records	Cause
January*	Maternal & Family Health	Provider	**461,070**	Ransomware
February	Reventics	Business Associate	**4,212,823**	Ransomware
March	Managed Care of North America	Business Associate	**8,861,076**	Ransomware
April	Pharmaca & BrightSpring	Provider	**5,815,591**	Ransomware
May	Point32Health (Tufts Health Plan, Harvard Pilgrim Health Care)	Health Plan	**2,624,191**	Ransomware
June **	El Centro Del Barrio d/b/a CentroMed	Provider	**350,000**	Ransomware
July	HCA	Business Associate	**11,270,000**	Hack
August ***	Purfoods	Provider	**1,229,333**	Ransomware
September ***	Temple University	Unnamed BA had breach	**430,381**	Hack
October	TruePill	Provider	**2,364,359**	Hack
November	Perry Johnson & Assoc.	Business Associate	**8,952,212**	Hack
December	23 and me ****	Other	**6,900,000**	Hack

Table 2. Largest new incidents by month, 2023 health data breaches

* Reported to Maine, but not HHS

** The three largest reports in June were associated with previously noted breaches: Intellihartx 4,898,430 from the Fortra/GoAnywhere incident, CareSource 3,180,537 which was affected by the MoveIT breach, and Harris County Hospital District d/b/a Harris Health System 455,676, which was also affected by the MoveIT breach.

*** Larger incidents in August and September included Colorado Department of Health Care Policy and Financing (HCPF) at 4,091,794, Maximus for 2,781,617, Oregon Health Plan for 1,700,000, Nuance for 1,225,054 and IBM with 630,755. All were related to the MOVEit breach.

**** 23andMe was a credential stuffing attack and the firm tried to claim users were responsible for reusing passwords.

An Addendum to 2022

The number of reported breaches that impacted less than 500 patients continue to dominate each year. Although this report is a retrospective of 2023 data, we would be remiss if we did not reference the HHS 2022 Annual Report to Congress, published February 22, 2024, where the "under 500" breaches reported consistently exceeds 60,000 per calendar year (Table 3).

Of the 63,966 "under 500" breach reports filed in 2022, 257,105 individuals were affected, with 91% of the reports received from healthcare providers, affecting 188,167 individuals (73%). The overwhelming cause of these breaches was unauthorized access or disclosure (59,727 reports, or 93%) affecting 171,100 individuals (67%).

Year	Under 500 Breaches Reported	500+ Breaches Reported	% Change in Under 500 Breaches Reported	% Change in 500+ Breaches Reported
2022	63,966	626	**+1%** ▲	**+3%** ▲
2021	63,571	609	**-4%** ▼	**-7%** ▼
2020	66,509	656	**+6%** ▲	**+61%** ▲
2019	62,771	408	**-.5%** ▼	**+35%** ▲
2018	63,098	302	--	--

Table 3. Largest new incidents by month, 2022 health data breaches

93% of breaches caused by Insider Unauthorized access

© Protenus 2024 | All Rights Reserved

Unauthorized access or disclosure can occur when sensitive information is shared with someone who does not have the authorization to view it. This could happen if an employee intentionally looks up patient data they have no reason to access (such as with snooping), accidentally sends confidential documents to the wrong email address, or if a hacker gains access to a company's database.

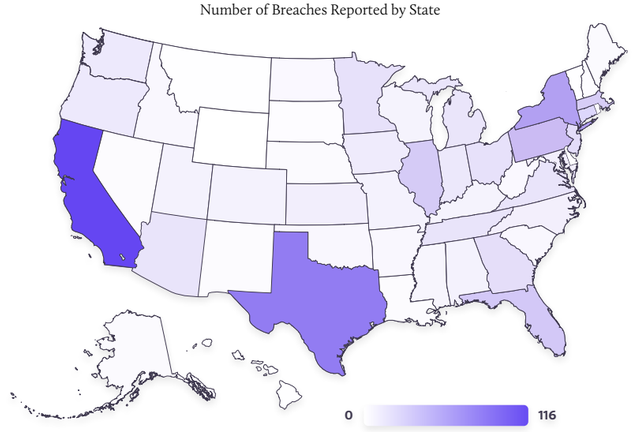
Unauthorized access often goes unnoticed since the number affected is not typically of high volume. Organizations often lack the technology resources to identify patterns of access by an individual that a human resource alone cannot identify proactively, given the sheer amount of data and activity produced by healthcare organizations daily.

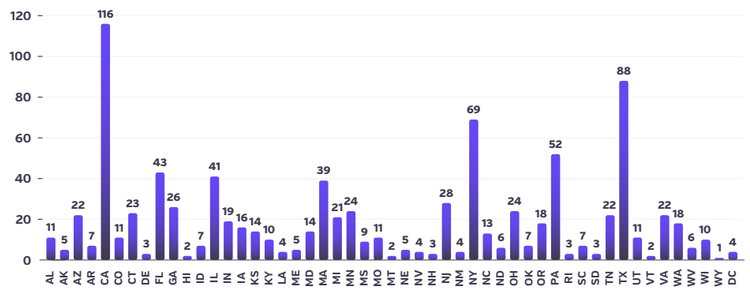
State Frequency

Our analyses determined that all 50 states were affected by data breaches in 2023 (Figures 3 and 4). California was the state with the most cases in 2023 with 116 reported, followed by Texas (88) and New York (69). Wyoming is the only state that had a single reported incident. One factor that may contribute to the higher frequencies in CA and TX could be that both states have publicly listed breach reports, which made us aware of incidents that would not necessarily show up on the HHS sites.

As in past years, each business associate breach was assigned just once to the state in which the business associate is headquartered, and was counted only once regardless of how many individual reports there were for the incident by its clients or covered entities. Therefore, Figures 3 and 4 shows the prevalence and frequency where disclosed breaches originated, leading to an underestimate of how many reports and records were involved for each state.

Figures 3 and 4.
Number of Breaches Reported by State





Who Reports Breaches?

As explained in the Methodology section, HHS's public breach tool indicates what type of entity reported the breach to them – a healthcare provider, a business associate, a healthcare clearinghouse, or a health plan. For the 735 reports of breaches affecting over 500 individuals submitted to HHS for calendar year 2023, Table 4 provides the breakdown by entity type.

It is clear that business associates accounted for the largest percentage of breached records reported to HHS for 2023 (57%). A similar analysis of reported entities could not be accurately performed for Breach Barometer data because in many cases, HIPAA covered entities were not the ones who reported a breach. In many cases, breaches were first reported by threat actors, researchers, or the media.

Our analysis shows breaches associated with business associates accounted for an even greater percentage of breached records, accounting for 69% or 118,069,903 of the 171,139,241 records compiled. This included all records reported by a business associate or where the breach was at the business associate, even if reported by some other entity.

Type of Entity	Number of Reports	Number of Records	% of All Reports	% of All Records
Provider	459	41,811,340	**62%**	**31%**
Health Plan	103	15,792,549	**14%**	**12%**
Clearing House	2	3,075	**< 1%**	**< 1%**
Business Associate	171	77,763,530	**23%**	**57%**
Total (Based on HHS data affecting >500 individuals)	735	135,370,494	--	--

Table 4. Largest new incidents by month, 2023 health data breaches

Since 2016 when we began the Breach Barometer, Protenus has been urging covered entities to pay greater attention to the security of their data held by or processed by business associates. At this point, it really shouldn't matter which entity reports the breach – we need to know whether the breach was at the business associate or at the covered entity, health plan, or healthcare clearinghouse.

Health Systems Overwhelmed by Attacks from All Sides

As stated earlier in this report, large health data ransomware attacks by hackers such as Cl0p were abundant in 2023. However, these external threats are not the only attack health systems need to worry about. While the majority of patient records were breached by hacking, the vast majority (93%) of overall incidents impacting 500 or less individuals investigated and reported by health systems were from insiders.

Although not mutually exclusive, hackers and business associates were associated with the greatest number of records breached in 2023. Breaches stemming from hacking and IT incidents, which include malware, ransomware and phishing attacks, have increased by more than 500% over the past decade, and make up a vast majority of reported breaches last year.

Hacking

Hacking incidents were up from 712 in 2022 to 768 in 2023, a modest increase of 8%. The number of records breached by hacking soared, however, from 51,395,517 in 2022 to 166,515,133 in 2023. Hacking incidents (including those involving business associates) accounted for 86% of all records in 2022; and a staggering 97% in 2023 (Figure 5).

Hacking incidents account for 97% of records breached

Unlike previous years where we reported sub-categories of hacking such as ransomware, email attacks, etc., in 2023 we are not breaking this information down because the initial method is not always disclosed by the reporting entity.

For historical comparison purposes, HHS's 2022 Report to Congress states hacking/IT incidents remained the largest category of breaches affecting 500 or more individuals occurring in 2022, comprising 74% of the reported breaches. In this same report, however, for breaches affecting less than 500 individuals in 2022, HHS reported that 93% of these breaches were caused by insider unauthorized access or disclosure (Figure 6). This is important to note as most of these breaches often go unnoticed or unreported, but may often lead to other types of incidents, or have more direct impact on individual patients and their privacy.

© Protenus 2024 | All Rights Reserved

Strategies to Reduce Attacks and Mitigate Risk

Hackers' tools and tactics continue to evolve, requiring healthcare organizations to stay on top of thorough risk assessments and provide effective, ongoing employee training especially considering the trends of staffing and budget constraints as well as merger and acquisition activity in the industry.

Delivering targeted education when healthcare employees improperly access patient data is 95% effective in preventing future misuse, and robust cybersecurity training can help protect employees from falling victim to social engineering, phishing attempts, and other ransomware attack vectors. Investing in automation and artificial intelligence can empower healthcare organizations to take a proactive stance on protecting patient data by enabling real-time intervention and targeted education.

To further mitigate data risks from attack, organizations should prioritize patch updates as well as backup and recovery strategies. When it comes to patch updates, some threat actors will attempt to exploit new vulnerabilities within a week or two after they are first reported. The longer the patch cycle, the more likely the threat actor will take advantage. Another way these threat actors attempt to profit is from ransomware attacks that encrypt patient data and systems to increase pressure on entities to pay for a decryption key. Research shows that entities that have current and usable backups that are stored offline are significantly less likely to pay ransom in the event they are attacked since they can more efficiently restore close-to-current data and squelch the attacker's demands.

Business Associates

The number of business associates, or outside people and organizations that perform work for entities covered by HIPAA like health plans or providers, are increasingly involved in data breaches. Similar to hacking related incidents, business associate breaches were also up in 2023, as are the number of breached records. In 2022, we reported 188 incidents involving business associates that accounted for 29,478,169 records. In 2023, we reported 238 incidents involving business associates that accounted for 118,069,903 records. Business associate breaches accounted for 69% of all breached records in 2023, up from 49% in 2022. Of those, 82% of the BA breaches were due to a hacking incident (Figure 7).

Figure 5.
Total Hacking Incidents

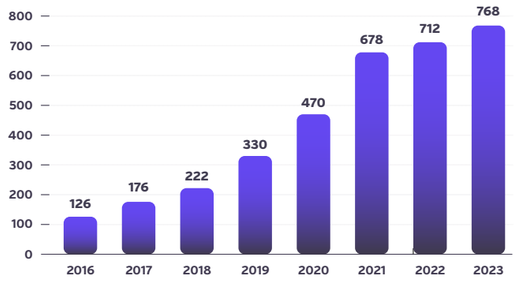


Figure 6.
HHS Office of Civil Rights Breach Reports of Unsecured PHI Affecting Fewer Than 500 Individuals in 2022 by % of Reports Received by type of Breach

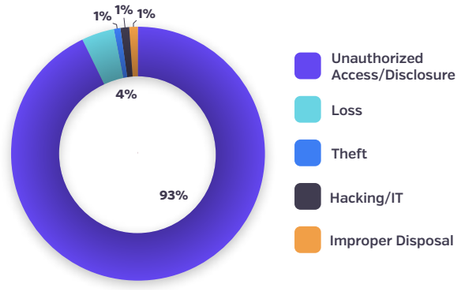
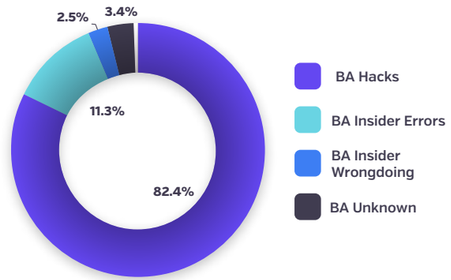


Figure 7.
Business Associate Breaches by Cause

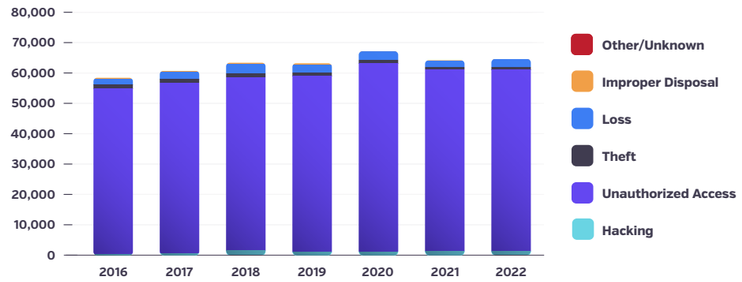


Insiders

In addition to hacking and business associate related breaches, the numbers involving threats and incidents from insiders continue. The number of insider errors was up slightly in 2023, but the number of records breached is down. The number of insider wrongdoing reports and records, which often involves shared credentials, snooping or peer/employee accessed records, was the lowest on record since we began reporting this information, with 32 reports involving 63,625 records in 2023.

Although the number of insider error and wrongdoing reported incidents are not at the extreme levels of hacking or BA related incidents in 2023, the majority of insider incidents often go unnoticed or unreported. As noted earlier, for breaches affecting less than 500 individuals in 2022, HHS reported that 93% of reports received were caused by unauthorized access or disclosure, and caused 22% of the breaches impacting more than 500 individuals affected.

Figure 8.
Breach Reported by Cause



When compared to prior years, unauthorized access, which includes insider incidents, continue to outpace all other causes for patient record breaches reported overall (Figure 8). Insider incidents can often lead to larger scale incidents, or have more direct impact on individual patients and their privacy. These incidents also have additional impact on the health organization, as patient trust and satisfaction may result in loss of business and reputational damage to the organization.

Breaches Left Undiscovered for 79 days

When examining all incidents with relevant data in 2023, on average, 79 days passed between the time a breach occurred to the time it was discovered (using arithmetic mean). (The "discovery date" is defined as the date that the third-party first discovered the breach — not the date that they first informed the covered entity about it.)

Our findings this year show a decrease in days of 21% from 2022, when the average time to discovery was 96 days. The average time from breach to discovery is important to point out because it gives an indication of how long patient data can be misused before organizations even realize it has been exposed and take remedial action. The median time it took to discover a breach was just 10 days, but it should be noted that there were a wide range of time frames for discovery throughout the year. The shortest time to discovery was one day, and the longest was more than 4 years.

One may argue that the time to discovery has been vastly shortened due to media or hackers making the breach public early on - less discreet than traditional methods of discovery from a covered entity or business associate. While long delays between a breach and its discovery is obviously of concern, there is also concern about the gap between when the breach occurred and when it was reported. For 2023, the average gap was 176.9 days (with a median of 83). For almost six months, threat actors may have been able to be misusing the data or leaking it publicly before patients are even notified. The extended amount of time often means patients are unaware their health information has been breached for several months, if not longer. In some cases in 2023, patients reported first finding out about breaches from the hackers or the media and not the covered entities or business associates.

Some entities and their legal counsel may claim that a breach was "discovered" when they finish their investigation and have determined who needed to be notified. We prefer HHS's definition of the date of discovery as when the entity or a reasonable person would have known or should have known they had a breach. Entities that do not follow HHS's definition of the date of discovery can lead to further violations as parties may exceed the 60 day rule of notification. Refer to 45 CFR §§ 164.400-414 HIPAA Breach Notification rule. For our analyses, if a vendor was involved, we used the date they discovered the breach as the discovery date and not the date they first notified the covered entity.

© Protenus 2024 | All Rights Reserved

With the massive amounts of data healthcare organizations process daily, human resources alone cannot efficiently identify all appropriate or inappropriate accesses to patient health records. Thus, it's not surprising that organizations that adopted technology as part of their patient privacy compliance efforts likely experienced a quicker time to identify a breach. IBM recently reported the cost of a healthcare data breach reached $10.9 million in 2023, and found that organizations "with extensive use of security AI and automation identified and contained a data breach 108 days faster than organizations with no use." Limited use of technology also made a significant impact, with an average time to identify and contain a breach in 234 days, which was 88 days shorter than organizations with no use. It's clear that even a limited effort to integrate AI technology into an organization's workflow can offer a significant return in the time to identify and contain a breach.

The Financial Burden of a Breach Intensified in 2023

On October 6, 2023, HHS announced annual inflation adjustments in the Federal Register, bringing about changes that Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and Privacy and Compliance Officers need to be aware of. These adjustments came into effect immediately and applied to all penalties assessed by the Office for Civil Rights (OCR) on or after this date. (It's important to note that these revised penalties are applicable only if the HIPAA violations occurred on or after November 2, 2015.)

The revised penalties reflect an increase from previous years, signifying a heightened emphasis on maintaining patient privacy. It is vital for healthcare organizations to understand these penalty revisions and take appropriate measures to avoid potential non-compliance fees. While regulatory compliance is a crucial aspect of patient privacy, it should not be the sole focus. All too often, hospital organizations fail to look at the bigger picture and overlook unauthorized access to PHI in the form of workforce policy violations that could ultimately result in insider errors or insider wrongdoing.

In 2023, penalties resulting from OCR investigations were notable. In November 2023, HHS and Montefiore Medical Center (MMC) entered into a Voluntary Resolution Agreement which included terms requiring MMC pay fines of $4,750,000. MMC also must implement corrective actions, following a multiyear investigation of the reported breach. The breach, which was reported to HHS by the healthcare organization on May 15, 2015 indicated "MMC discovered that from January 1, 2013 through June 30, 2013, one of its employees inappropriately accessed patient account information, including the patient's name, address, SSN, next of kin, and health insurance information, of 12,517 patients from its electronic medical record system and then sold certain patient information to an identity theft ring. On November 23, 2015, HHS notified MMC that it was initiating an investigation regarding MMC's compliance with the HIPAA Rules."

Although the MMC settlement was most notable given the penalty dollar amount, at least 12 other resolution agreements or settlements occurred in 2023 in which an OCR investigation indicated a healthcare entity was in potential violation of the HIPAA Privacy or Security Rule and were required to perform corrective action plans and payments associated with financial penalties. As of December 31, 2023, OCR settled or imposed a civil money penalty in 141 cases resulting in a total dollar amount of $137,738,772.00, since the compliance date of the Privacy Rule in April 2003.

The OCR is not the only one enforcing privacy and security regulations. States including NY, NJ, CA, IN, GA, PA and OR all announced settlements in 2023. One such example was in Sept. 2023, California Attorney General Rob Bonta announced a settlement with Kaiser Foundation Health Plan, Inc., and Kaiser Foundation Hospitals (collectively "Kaiser") resolving allegations that the healthcare provider "unlawfully disposed of hazardous waste, medical waste, and protected health information at Kaiser facilities statewide." As part of the settlement, Kaiser was liable for a total of $49 million.

It's important to note that the cost of a breach goes well beyond HHS or state penalties. Reputational damage, loss of business and other fines associated with operational process changes and corrective actions add to the tab,with some estimations reaching close to $11M. According to IBM's Cost of a Data Breach 2023, "Healthcare continues to experience the highest data breach costs of all industries, increasing from USD 10.10 million in 2022 to USD 10.93 million in 2023—an increase of 8.2%. Over the past three years, the average cost of a data breach in healthcare has grown 53.3%, increasing more than USD 3 million compared to the average cost of USD 7.13 million in 2020. Since the start of the COVID-19 pandemic, the industry has seen notably higher average data breach costs."

Evolution of the CISO: A Key Stakeholder

If (or when) the New York Governor's cybersecurity regulation we mentioned earlier in this report passes, every hospital in the state will be required to have a Chief Information Security Officer (CISO) that will enforce the cybersecurity policies and to annually review and update them as needed. The role of a security official for a covered entity in itself is nothing new, and is consistent with the HIPAA Security rule §164.308 to "identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity." The only difference it appears in the proposed New York regulation is the requirement that the role be elevated to a C-level. And, although CISOs are not new to healthcare, the requirement of the role will most certainly impact some hospital organizations. Will other states follow?

Today, the realities of cybersecurity and regulatory compliance requirements call for an information security leader who can provide a focused, comprehensive approach to protecting sensitive information and systems. In the world of healthcare, CISOs face a myriad of added challenges, where disruptive cyberattacks do more than threaten the organization's reputation and bottom line—they can also impact the ability to deliver life-saving services and treatment to the organization's patients. This added level of pressure has created an increased intensity that requires today's CISO be laser focused on areas that extend beyond cybersecurity and compliance regulations. Partnering with other healthcare and compliance stakeholders within the organization to develop proactive methods of risk management can help to support a robust cyber resilient program.

To address this issue comprehensively, CISOs and healthcare compliance professionals must work together on a proactive approach that goes beyond mere IT or regulatory compliance. This includes implementing comprehensive privacy policies and regularly reviewing them to ensure they align with the evolving landscape of patient privacy. A comprehensive healthcare compliance program should include the following key elements:

Privacy Policies and Procedures

Develop and maintain comprehensive privacy policies and procedures that outline how patient information should be handled, stored, and shared. Regularly review and update these policies to address new privacy risks and ensure compliance with regulatory requirements.

Training and Education

Provide regular training and education to employees on patient privacy best practices, the importance of safeguarding PHI, and the potential consequences of policy violations. This will help create a culture of privacy and ensure that all staff members understand their responsibilities.

Monitoring and Auditing

Implement robust monitoring and auditing processes to detect and address any unauthorized access or use of patient information. AI-driven healthcare compliance analytics can play a crucial role in identifying patterns and anomalies proactively - that may indicate potential policy violations.

Incident Response Plan

Develop a comprehensive incident response plan that outlines the steps to be taken in the event of a privacy breach or policy violation. This plan should include procedures for investigating incidents, notifying affected individuals, and mitigating any potential harm.

Continuous Improvement

Regularly review and assess the effectiveness of the healthcare compliance program and make necessary improvements to address any identified weaknesses or gaps. This will ensure that your organization stays up-to-date with the evolving landscape of patient privacy.

Annual Risk Analysis

Perform a comprehensive risk assessment of the organization's privacy and security posture and programs, identifying gaps in those programs, along with the related risk management status of the organization. The risk analysis must also set forth the plans for mitigation of the identified gaps to reduce the identified risks.

© Protenus 2024 | All Rights Reserved

Brief Summary of OCR Actions

Special Section

The HHS OCR routinely reports on the status of complaints and audit reviews, for those received by the department. According to the HHS HIPAA Enforcement Highlights website, as of Dec. 31, 2023, ***"Since the compliance date of the Privacy Rule in April 2003, OCR has received over 348,877 HIPAA complaints and has initiated over 1,182 compliance reviews. We have resolved ninety-nine percent of these cases (345,998)."*** From the compliance date to the present, the compliance issues most often alleged in complaints are, compiled cumulatively, in order of frequency:

- **Impermissible uses and disclosures of protected health information;**
- **Lack of safeguards of protected health information;**
- **Lack of patient access to their protected health information;**
- **Lack of administrative safeguards of electronic protected health information; and**
- **Use or disclosure of more than the minimum necessary protected health information**

In 2023, ransomware groups posted explicit photos of named plastic surgery patients with their medical records and contact information, and then contacted the patients directly to extort personally or harass. Additionally, there have been instances where law firms that held sensitive medical information on clients were hacked and their data dumped on the dark web.

Findings Highlight Lack of Controls

Most often, OCR has reported that the lack of controls or comprehensive risk assessment are the top security issues and violations that may impact patient privacy. Melanie Fontes Ranier, Director at the U.S. Department of Health and Human Services Office for Civil Rights, Washington, DC was interviewed for an article published in the September 2023 issue of HCCA's Compliance Today, stating "In our investigations, the most common compliance issues and violations we see are regulated entities failing to conduct a risk analysis, perform risk management, and implement access controls to prevent the wrong people from gaining access to electronic (ePHI), as well as failing to implement audit controls to examine activity in the information system and other basic requirements of the HIPAA Security Rule." Also mentioned in the article was the need for HIPAA covered entities to ensure they have adequate business associate agreements in place when working with other vendors, to help ensure proper handling and securing of patient data.

OCR Trending Now

2023 was a year fueled by political and personal turmoil, leaving many patients fearful that their medical records would be exposed in ways they never wanted to imagine. In 2023 HHS published a number of Notices of Proposed Rulemaking (NPRMs) that aim to further strengthen the HIPAA Privacy Rule protections specific to areas including but not limited to LGBTQ+, reproductive health, and substance abuse. Government enforcements such as these further highlight the sensitivity of patient information, and the importance of patient privacy rights.

In December 2023, OCR published a concept paper outlining plans to improve cyber resiliency and protect patient safety. According to the OCR announcement, cyber incidents in healthcare are "on the rise", stating from 2018-2022 there has been a 93% increase in large breaches reported to OCR (369 to 712), with a 278% increase in large breaches involving ransomware. Cyber incidents affecting hospitals and health systems have led to extended care disruptions, patient diversions to other facilities, and delayed medical procedures, all putting patient safety at risk."

And finally, just days before the publication of this Breach Barometer report, HHS OCR made two notable announcements worth mentioning here.

First, OCR announced that it will be conducting a HIPAA Audit Review Survey to seek feedback from entities that were subjects of HIPAA compliance audits between 2016-2017 to obtain feedback on the audit process and impact on the entities' day-to-day business operations so that the OCR can improve future audit programs. The aim is to determine the efficacy of the audit program in assessing the efforts made by HIPAA-covered entities and their business associates to comply with the HIPAA rules and measure the effect of the audits on covered entities' and business associates' subsequent actions to comply with HIPAA. The survey will consist of 39 questions, and will be collected via an online portal.

The second announcement sends a clear message to healthcare organizations and their partners as HHS announced its second-ever settlement of a ransomware attack. The announcement states, "Ransomware and hacking are the primary cyber-threats in health care. Over the past five years, there has been a 256% increase in large breaches reported to OCR involving hacking and a 264% increase in ransomware. In 2023, hacking accounted for 79% of the large breaches reported to OCR. The large breaches reported in 2023 affected over 134 million individuals, a 141% increase from 2022."

© Protenus 2024 | All Rights Reserved

Conclusion

In 2023, the number of patient records compromised in data breaches is up 187% from prior year, and over 320% since 2020.

The healthcare industry saw an unprecedented number of hacking and business associate incidents while insider errors continued to compromise millions of records. Threat actors will continue to hone their cyberattack methods and find new ways to violate healthcare's inadequate, scattered breach defenses, possibly finding deeper success in recruiting burned-out or disgruntled staff and to grant them insider access, or soliciting various forms of ransom payment from innocent patients when their sensitive data is breached. We also expect to see more supply chain or vendor attacks that will give threat actors access to even larger amounts of protected health data. And, with 93% of incidents reported that include less than 500 individuals coming from insiders, hospitals not only need to protect health data from external threats, but must be just as vigilant with those within its own organization.

With an astounding 171 million records breached in 2023, it's more evident than ever that healthcare's reliance on technology and critical need to access and protect massive volumes of patient data every day will continue to drive these trends and create challenges for the entities that generate and store sensitive patient data.

Key Insights

Hackers will persist in launching large-scale attacks, while insider threats will continue to disrupt operations covertly. Additionally, financial pressures on organizations will intensify due to increasing enforcement and rising fines.

Cybersecurity makes way for cyber resiliency, a concept that combines business continuity, information system security and healthcare organizational resilience together. Organizations must continue to deliver on patient care and other intended business outcomes despite the challenges set forth by hackers and other cyber attacks. Actions such as those from OCR, the New York Governor and other states' leaders to strengthen cyber resiliency may likely be the pattern we see increase in 2024. Organizations must continue to be wakeful in their efforts to tighten the reins on patient privacy and security measures. Even with more robust regulations, the bigger challenge may be in developing methods to outsmart the threat actors, including those inside the organization, and beat them at their game.

Get Defensive and Take a Proactive Approach

It's not if hacker incidents or insider threats will occur, but rather it's when and with what impact. Organizations must set forth a defense plan to prevent an attack from occurring so they can better protect their systems, their data and ultimately their patients. HIPAA covered entities and their business associates cannot rely on manual or reactive posture to identify patient record access. Healthcare leaders must take a proactive approach and prioritize cyber resiliency, policy education, and invest in technology that offer modern safeguards and efficiencies into real-time breach detection and prevention, monitoring every single access to every patient record, every day. Only then can they better protect patients and mitigate risk organization-wide.

What 2024 will bring is yet to be known, however, we do know that there are programs organizations can implement described earlier in this report that can help mitigate otherwise costly risk.

About Protenus

The Protenus healthcare compliance analytics platform harnesses the power of artificial intelligence to audit every access to patient records for the nation's leading health systems, providing healthcare leaders full insight into how health data is being used, and alerting privacy, security, and compliance teams to inappropriate activity. Protenus helps our partner hospitals transition from a reactive posture to a proactive posture that focuses on risk reduction and prevention, better protecting their data, their patients, and their institutions. We are committed to innovation, determined to reduce risk, and focused on supporting our community of employees, customers, and ultimately, patients. Empowering healthcare to eliminate risk is at the heart of all we do. Protenus was awarded Best in KLAS 2023 and 2024 for both patient privacy monitoring and drug diversion surveillance solutions, is a three-time winner of Forbes' Best Startup Employers, named one of 2021 CBInsights Digital Health 150, named one of The Best Places to Work in Healthcare by Modern Healthcare and one of the Best Places to Work in Baltimore by the Baltimore Business Journal and the Baltimore Sun. Learn more at protenus.com and follow us on X @Protenus.

About DataBreaches.Net

DataBreaches.net is a website devoted to reporting on data security breaches, their impact, and legislative developments relevant to protecting consumer and patient information. In addition to providing news aggregation from global sources, the site also features original investigative reporting and commentary by the site's owner, a healthcare professional and privacy advocate who writes pseudonymously as "Dissent."

© Protenus 2024 | All Rights Reserved

Methodology

The purpose of this section is to explain decisions that were used to guide the analyses. Incidents were compiled and analyzed for Protenus by DataBreaches.net, with additional material and analyses provided by Protenus.

It should be understood that the Breach Barometer uses a coding system different from that used by HHS in its breach reporting tool. The coding system used for this report distinguishes healthcare employee events from external actor incidents, and it encompasses incidents involving health-related or medical information about U.S. residents or citizens — whether or not it impacts a HIPAA covered entity. Additionally, whereas the HHS breach portal may show multiple entities reporting the same incident, the Breach Barometer counts those multiple reports as a single new incident.

Each year has posed new challenges and issues for patient privacy, and 2023 was no different in those respects. For those already familiar with our methodology, here are two noteworthy differences from previous years:

Rather than becoming more transparent in disclosures, many entities sought new ways to keep us all in the dark. Instead of simply reporting they suffered a ransomware attack, many reported they were investigating a "cybersecurity incident." Many disclosure notices did not clearly indicate whether data had been encrypted, whether there had been any ransom demand, and whether any ransom had been paid. When in doubt as to whether an incident involved data encryption or not, we coded incidents as "hacking." The hacking statistics contain incidents that involved ransomware. Similarly, some incidents coded as "ransomware" may not have involved encryption of data as many ransomware groups reverted to simply exfiltrating data and then demanding payment to delete it from their servers.

Victims often had trouble determining whose protected health information was affected and who needed to be notified. The regulations give entities 60 calendar days from discovery of a reportable breach to disclose the breach to HHS and to those affected. All too often, however, entities did not or could not comply with that timeframe. In 2023, we recorded a number of instances where entities submitted "500" or "501" as markers to indicate that they knew more than 500 patients or members were affected but did not have the total number yet. As readers will learn in the results portion of this report, the vast majority of markers never got updated by the end of 2023.

Sources of Data

Incidents were included in our analyses if they involved health-related or medical information about U.S. residents or citizens and if the incident was first disclosed between January 1, 2023 and December 31, 2023. Collection of reports stopped on January 27, 2024, even though we realize some reports from 2023 came in after that.

As in our past reports, not all entities included in our analyses are medical entities or HIPAA-covered entities. While our analyses include incidents that appear on the U.S. Department of Health & Human Services public breach list, other sources included:

- Incidents reported to state regulators when such reports could be found online. For 2023, we did not have reports from the Maryland Attorney General's Office for the full year as they had not updated their site past April when we stopped data collection for the year. That left us with fewer reports from that source than we had last year or that we would have if their full database was available for the year.
- Incidents based on investigative journalism by DataBreaches.net that may not have been reported to federal or state regulators. These Incidents include verified data leaks discovered by researchers as well as confirmed breaches by threat actors that were not or had not yet been disclosed to regulators.

Coding of Incidents

The Breach Barometer uses a coding system different than that used by HHS's public breach tool:

- HHS codes some incidents as "unauthorized access/disclosure." That category could include incidents of insider wrongdoing/snooping, but it could also include external threat actors or just misconfigured databases that expose information. The Breach Barometer's coding system distinguishes insider/employee events from external actor incidents and includes misconfiguration-based exposures or leaks as "Insider-Error."
- HHS's category "Hacking/IT Incident" could mean an external hack, but it could also mean any other type of IT incident that might not involve an external threat actor. The Breach Barometer uses the "Hack" category for external threat actors, and where known, we provide additional data on whether the attack involved email (as in phishing) or extortion (as in ransomware) demands. Because most entities generally do not provide a lot of details about the attacks, readers who tend to be conservative in interpreting analyses may feel safer just using the total number for the overall hacking category..

As we have done in the past, in the event of a breach involving a vendor or Business Associate, we counted that as (only) one new incident, even if there are dozens of covered entities reporting it to patients or regulators. What HHS may show as seven reports, and what other analyses may report as seven breaches, the Breach Barometer counts as 7 reports but only 1 new incident.

In 2023, there were some massive breaches involving attacks on business associates or vendors such as incidents involving hacks on entities using MOVEit software and GoAnywhere software. There were also breaches involving law firms that affected millions of patients. But despite all the reports that came in during the year, our estimates of the number of breaches involving business associates is almost certainly a significant underestimate because:

- Not all affected entities name or even note a business associate or vendor in their breach reports to HHS or the public. This year, DataBreaches.net made a point of checking every entry on HHS's public breach tool to see if those reporting as a Provider, Health Plan, or Clearing House indicated a Business Associate was involved. Somewhat to our surprise, we found many incidents involved unnamed vendors even when the covered entity's disclosure made no mention of any vendor, and
- When some business associates report incidents to regulators, they may not specify how many covered entities or patients are included in their report, leaving us wondering whether their reported numbers include numbers reported directly by some of their clients and whether all individuals are patients.

"Insider-Error" or "Insider-Wrongdoing?"

Occasionally, we did not have enough information to determine whether a breach involving employees was accidental or not. When protected health information (PHI) is disposed of improperly, it may be an accident involving a crew or contractor, or it may be that someone got lazy and didn't care enough and knew what they were doing was wrong. Thus, the "insider-wrongdoing" category includes snooping, criminal behavior incidents (such as ID theft involving patient data), but also other willful misbehaviors that result in HIPAA violations.

In 2023, some entities disclosed that they had been using trackers on portions of their websites that transmitted PHI to other entities. DataBreaches.net and Protenus decided to treat such tracking as "Insider-Error" and gave entities the benefit of the doubt as to their intentions.

Who Reports Incidents?

HHS's public breach tool contains a field that indicates what type of covered entity reported the incident in their records – either a provider, a business associate, a clearing house, or a health plan. But the Barometer includes entries where neither the breached entity nor any associated entity first reported the incident. For the Barometer's purposes, an incident may be listed under "Provider" because the incident was at the provider's, even though it may have first been reported by the media. In many cases, threat actors were actually the first to disclose a breach.

Calculating Gap to Discovery and Gap to Reporting

How long did it take for breaches to be discovered, and how long did it take for breaches to get reported or disclosed publicly? The inclusion of numerous third-party incidents resulted in the decision that for purposes of determining time intervals for "date of the breach to date of discovery" and "date of discovery to date of the public report," we would define the "discovery date" as the date that the third party first discovered the breach and not the date that they first informed the covered entity about it (even though covered entities may acceptably use the date they were first informed as the date of discovery in starting a 60-day clock to notify). As in past years, if we only knew the month or year the breach first occurred, we used the first day of the month or year in our calculations.

In calculating time intervals between the date of the breach and the date of the public report, we defined the date of the public report as the date that the entity reported the incident to HHS or a regulator, sent letters to affected patients or members, or issued a press release. We note that in many cases, the entity's public disclosure might be months after threat actors, researchers, or the media first disclosed breaches. It may also be months after patients' protected health information may have been dumped on the dark web by threat actors whose ransom demands were ignored or refused.

As in 2022, we noted that many entities treated the date that they confirmed PHI was involved in an incident or the date that they finished their investigation as their "date of discovery." As we understand it, that is not compliant with HIPAA and HITECH, but HHS has not taken any enforcement action on this issue as of the time of this report.

State Frequency Data

For state frequency data, if a Business Associate or vendor was responsible for the breach, we entered one report into the state frequency counter for the first entity that disclosed the breach, but we did not enter all the covered entities' states that month or in subsequent months. Thus, the state frequency map is not a frequency map for all reports but a frequency map of the first report of new incidents. A breach involving a business associate got charged to the state where the business associate is headquartered if we knew the identity of the business associate.

For Further Information on Methodology

Any inquiries about the data collection or analyses should be directed to **marketing@protenus.com.**

Disclaimer

This report is made available for educational purposes only and "as-is." Although we have tried to provide accurate information, as new information or details become available, any findings or opinions in this paper may change. Despite our diligent efforts, we remain convinced that the breaches we find out about publicly are only the tip of a huge iceberg.

© Protenus 2024 | All Rights Reserved