SECURITY BREACHES IN HEALTHCARE IN 2023

Published: January 31, 2024

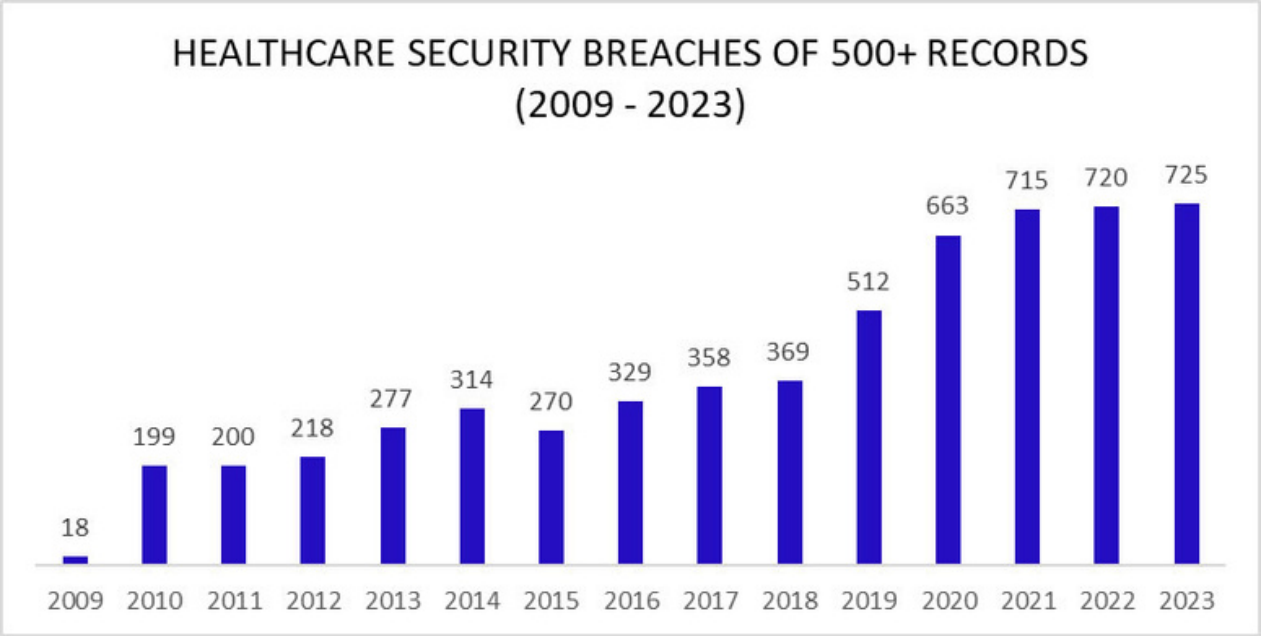
THE HIPAA JOURNAL

Please see updates on this page:

https://www.hipaajournal.com/security-breaches-in-healthcare/

SECURITY BREACHES IN HEALTHCARE IN 2023

An unwanted record was set in 2023 with 725 large security breaches in healthcare reported to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR), beating the record of 720 healthcare security breaches set the previous year. Aside from 2015, the number of reported security breaches in healthcare has increased every year although the rate of increase is slowing and 2024 could see the healthcare industry start to turn the corner.



As the chart shows, healthcare security breaches are occurring twice as often as in 2017/2018, with two large healthcare data breaches reported each day on average in 2023. Just a few years ago it was alarming that large healthcare data security breaches were being reported at a rate of one a day. Little did we know how bad the situation would get in such a short space of time.

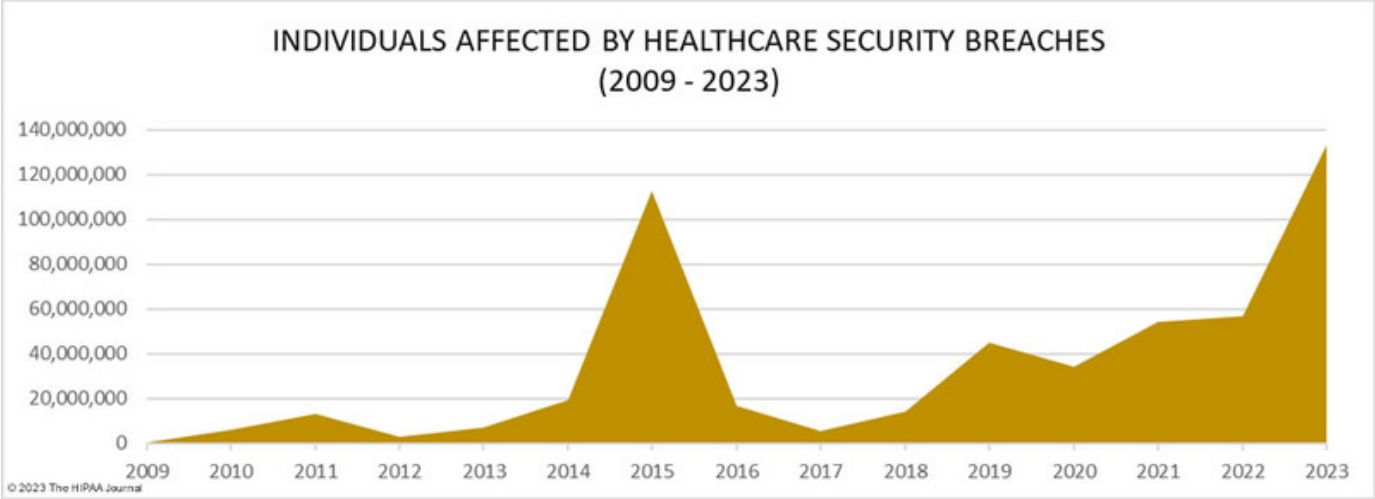
The healthcare industry is struggling to deal with increasingly sophisticated cyberattacks, although in many incidents cyber threat actors have exploited vulnerabilities that should have been identified and addressed long before they were found and exploited by hackers. Many healthcare organizations are failing at basic security measures and are not consistently adhering to cybersecurity best practices due to budgetary pressures, difficulty recruiting and retaining skilled IT security professionals, and confusion about the most effective steps to take to improve resilience to cyber threats.

With healthcare data breaches increasing year-over-year, something needs to be done to help healthcare organizations improve resilience to cyber threats and action is now being taken at the state and federal levels. In December 2023, the HHS published a concept paper outlining plans to improve resilience to cyber threats across the sector and limit the severity of attacks when defenses are breached. In the paper, the HHS indicated it will be adopting a carrot-and-stick approach by developing voluntary Healthcare and Public Health (HPH) Sector Cybersecurity Goals (CPGs) that consist of cybersecurity measures that will have the greatest impact on security along with an update to the HIPAA Security Rule to add new cybersecurity requirements.

In January 2024, the CPGs were unveiled. They consist of Essential CPGs, which are high-impact, low-cost steps that healthcare organizations can take to improve cybersecurity, and a set of Enhanced CPGs to help healthcare organizations mature their cybersecurity programs. The HHS also hopes to obtain the necessary funding to help low-resourced healthcare delivery organizations cover the initial cost of the cybersecurity improvements in the Essential CPGs and to create an incentive scheme to encourage the adoption of the Enhanced CPGs.

In response to an alarming increase in cyberattacks on New York hospitals, New York Governor Kathy Hochul announced new cybersecurity measures had been proposed for New York hospitals, which are expected to be finalized in the first half of 2024. Hospitals in the state will be given a 1-year grace period to comply with the new requirements and funding has been set aside to help them cover the cost of making the necessary improvements.

It is not just the increasing number of data breaches that is a cause of concern it is the scale of these data breaches. 2023 was the worst-ever year for breached healthcare records with breached records increasing by 156% from 2022 to 133,068,542 breached records, beating the previous record of 113 million records set in 2015. In 2023, an average of 373,788 healthcare records were breached every day.



The total of 133 million records is also likely to significantly increase. To meet the breach reporting requirements of the HIPAA Breach Notification Rule, OCR must be notified within 60 days of the discovery of a data breach. When that deadline is near and breached organizations have not yet completed their document reviews to find out how many individuals have had their protected health information (PHI) exposed, breaches are reported to OCR using a placeholder of 500 or 501 records.

The breached entity can then amend its OCR breach report when the number of affected individuals has been confirmed. Currently, 54 data breaches in 2023 are listed on the OCR breach portal as affecting 500 or 501 individuals. Some of these incidents have been reported by large healthcare providers, health plans, and business associates, so some of those breaches could involve hundreds of thousands or even millions of records.

Biggest Healthcare Security Breaches in 2023

Since several large healthcare organizations and major vendors have yet to confirm how many individuals have been affected by data breaches, the list of the biggest healthcare data breaches in 2023 is subject to change. Based on current figures, 114 data breaches of 100,000 or more records were reported in 2023, including 26 data breaches of more than 1 million records, 5 data breaches of more than 5 million records, and one breach of 11.27 million records.

SECURITY BREACHES IN HEALTHCARE IN 2023

The average data breach size in 2023 was 183,543 records and the median data breach size was 5,175 records.

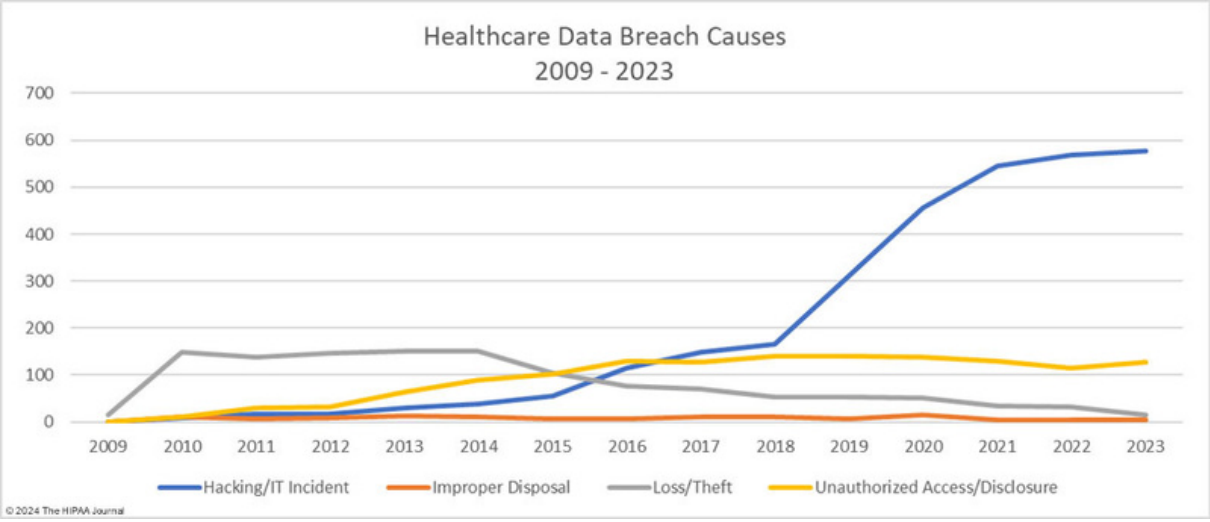
Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Cause of Data Breach
HCA Healthcare	TN	Business Associate	11,270,000	Hackers accessed an external storage location that was used to automatically format emails
Perry Johnson & Associates	NV	Business Associate	8,952,212	Hackers access to its network between March 27, 2023, and May 2, 2023
Managed Care of North America (MCNA)	GA	Business Associate	8,861,076	Ransomware attack with data leak (LockBit ransomware group)
Welltok, Inc.	CO	Business Associate	8,493,379	MOVEit Transfer vulnerability exploited (Clop hacking group)
PharMerica Corporation	KY	Healthcare Provider	5,815,591	Ransomware attack with data leak (Money Message ransomware group)
HealthEC LLC	NJ	Business Associate	4,452,782	Hackers had access to its network between July 14, 2023, and July 23, 2023
Reventics, LLC	FL	Business Associate	4,212,823	Ransomware attack with data leak (Royal ransomware group)
Colorado Department of Health Care Policy & Financing	CO	Health Plan	4,091,794	MOVEit Transfer vulnerability exploited at a vendor (Clop hacking group)
Regal Medical Group, Lakeside Medical Organization, ADOC Acquisition, & Greater Covina Medical Group	CA	Healthcare Provider	3,388,856	Ransomware attack with data leak (Unspecified, Russia-based ransomware group)
CareSource	OH	Business Associate	3,180,537	MOVEit Transfer vulnerability exploited (Clop hacking group)
Cerebral, Inc	DE	Business Associate	3,179,835	Impermissible disclosure of PHI via Pixel tracking code on its website
Nations Benefits Holdings, LLC	FL	Business Associate	3,037,303	Fortra GoAnywhere MFT vulnerability exploited (Clop hacking group)
Maximus, Inc.	VA	Business Associate	2,781,617	MOVEit Transfer vulnerability exploited (Clop hacking group)
ESO Solutions, Inc.	TX	Business Associate	2,700,000	Ransomware attack (ransomware group unknown)
Harvard Pilgrim Health Care	MA	Health Plan	2,624,191	Ransomware attack (ransomware group unknown)
Enzo Clinical Labs, Inc.	NY	Healthcare Provider	2,470,000	Ransomware attack (ransomware group unknown)
Florida Health Sciences Center, Inc. dba Tampa General Hospital	FL	Healthcare Provider	2,430,920	Ransomware attack (Snatch and Nokoyawa groups claimed credit)
Postmeds, Inc.	CA	Healthcare Provider	2,364,359	Hackers hack access to its network between August 30, 2023, and September 1, 2023
Centers for Medicare & Medicaid Services	MD	Health Plan	2,342,357	MOVEit Transfer vulnerability exploited at Maximus Inc. (Clop hacking group)
Arietis Health, LLC	FL	Business Associate	1,975,066	MOVEit Transfer vulnerability exploited (Clop hacking group)
Pension Benefit Information, LLC	MN	Business Associate	1,866,694	MOVEit Transfer vulnerability exploited (Clop hacking group)
Performance Health Technology	OR	Business Associate	1,752,076	MOVEit Transfer vulnerability exploited (Clop hacking group)
Prospect Medical Holdings, Inc.	CA	Business Associate	1,309,096	Ransomware attack and data leak (Rhysida group unknown)
PurFoods, LLC	IA	Healthcare Provider	1,229,333	Hackers had access to its network between January 16, 2023, and February 22, 2023
Virginia Dept. of Medical Assistance Services	VA	Health Plan	1,229,333	Hacking incident - details unknown
Nuance Communications, Inc.	MA	Business Associate	1,225,054	MOVEit Transfer vulnerability exploited (Clop hacking group)

Causes of Cybersecurity Breaches in Healthcare in 2023

There has been a leveling off of security breaches in healthcare in the last three years after a sharp increase in hacking incidents between 2018 and 2021, with only a 0.69% year-over-year increase in large data breaches. The year included two major mass hacking incidents by the Clop hacking group that affected many healthcare organizations. Clop-linked threat actors exploited zero-day vulnerabilities in two file transfer solutions – Fortra's GoAnywhere MFT and Progress Software's MOVEit Transfer. The first of these mass hacking incidents occurred in January with the group exploiting a remote code execution flaw – CVE-2023-0669 – in GoAnywhere MFT to attack almost 130 organizations, including healthcare organizations and business associates.

The second mass hacking incident occurred in May and was far more extensive. A zero-day vulnerability was exploited in MOVEit Transfer and more than 2,470 organizations had data stolen from their MOVEit servers. Across those incidents, the data of more than 94 million individuals was stolen. Many healthcare providers and business associates were affected, and the top three worst affected companies were HIPAA-regulated entities – Maximus, Welltok, and Delta Dental of California and Affiliates.

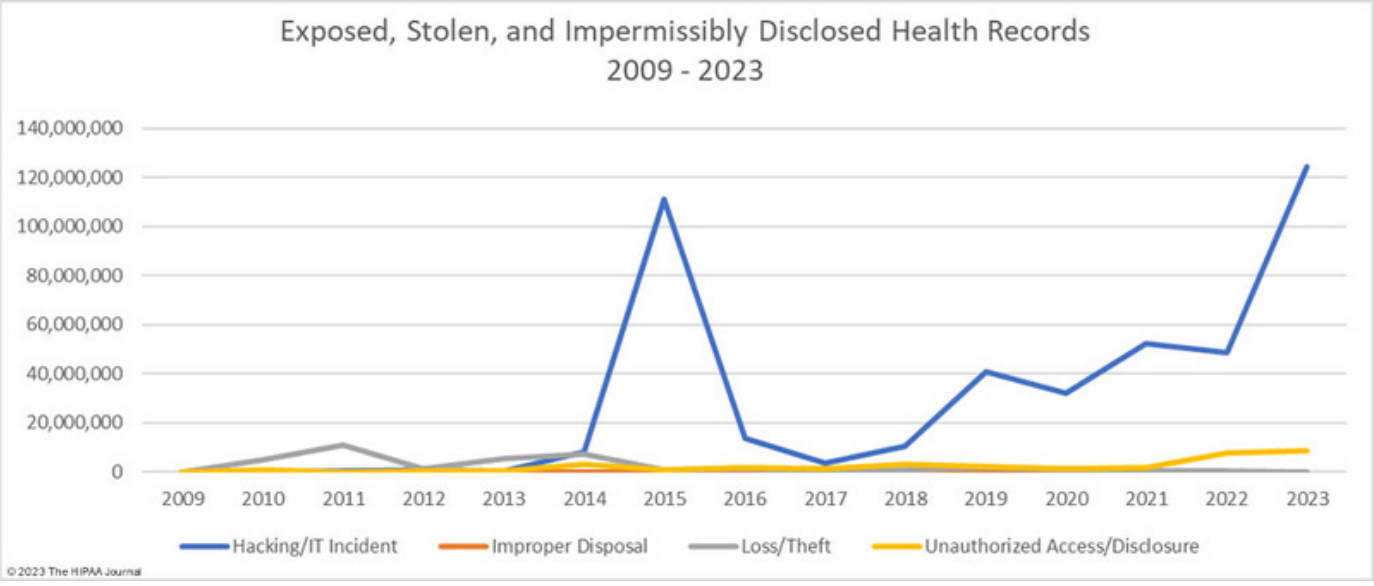
As the graph below shows, hacking incidents continue to dominate the breach reports with almost four times as many hacking incidents reported in 2023 than all other breach causes combined. 578 of the year's 725 breaches were due to hacking and other IT incidents.



The sharp rise in hacking incidents in 2018 is linked to the widespread use of ransomware and the proliferation of ransomware-as-a-service (RaaS) groups, which allowed attacks to be conducted at scale by recruiting affiliates to breach networks and receive a cut of any ransoms generated.

Data from the ransomware remediation firm Coveware shows ransomware attacks are becoming much less profitable, with fewer victims choosing to pay the ransom. In Q4, 2023, 29% of ransomware victims paid the ransom compared to 85% at the start of 2019. In these attacks, ransomware groups steal vast amounts of sensitive data. If the ransom is not paid, the data is leaked or sold to other threat actors and is used for a multitude of nefarious purposes, but it is ransom payments that are the main source of income for these groups, and with fewer ransoms being paid, ransomware actors need to conduct more attacks to maintain their incomes.

The number of healthcare records stolen in hacking incidents has increased sharply in recent years. In 2023, more than 124 million records were compromised in healthcare hacking incidents which is 93.5% of the year's total number of breached records.



On average, 215,269 healthcare records were stolen in each hacking incident (median 73,623 records).

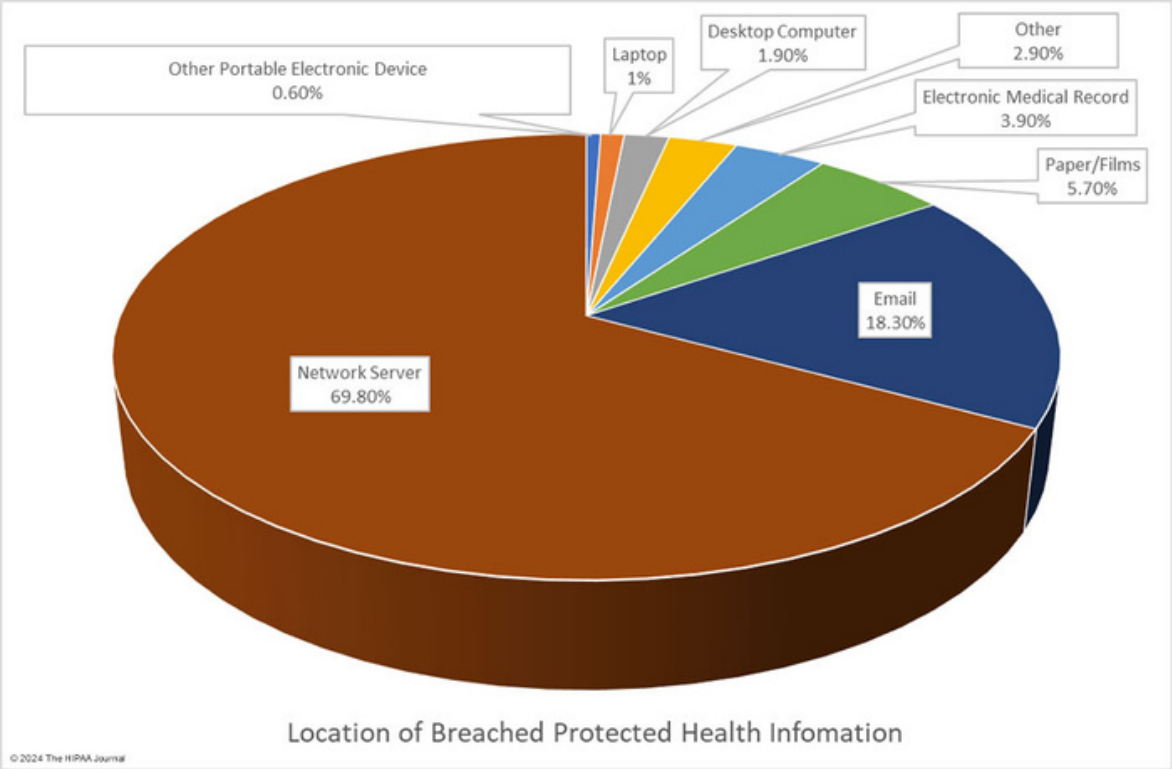
The scale of some of these hacking incidents emphasizes the need for network segmentation to limit the data that can be accessed if networks are breached, and the importance of implementing a zero trust architecture. Zero trust assumes that adversaries have already breached 'perimeter' defenses and requires verification and validation of every stage of a digital interaction.

Aside from hacking incidents, there are several other types of security breaches in healthcare. There was a 10.4% increase in unauthorized access and disclosure incidents in 2023 and a 13.6% increase in impermissibly accessed or disclosed records. 127 Unauthorized access/disclosure incidents were reported in 2023 and 8,598,916 records were accessed or disclosed across those incidents.

These HIPAA breaches may be smaller than the hacking incidents, averaging 67,708 records per incident (median 1,809 records), but they can be just as harmful.
Improper disposal incidents have remained consistently low over the past 5 years (5 incidents in 2023) apart from a spike during the pandemic in 2020, and there has been a marked decline in loss/theft incidents, of which there were only 15 incidents reported in 2023 – the lowest total of any year to date. The fall in these incidents can be explained by the widespread use of encryption on portable electronic devices and the migration of data to the cloud.

Given the high percentage of hacking incidents, the most common locations of breached PHI – network servers – should come as no surprise. In 2023, 69.8% of large data breaches involved network servers (506 incidents). Email was the next most common location of compromised PHI, accounting for 18.3% of breaches (133 incidents).

While multifactor authentication does not provide complete protection against email account breaches, widespread adoption of phishing-resistant multifactor authentication will see email data breaches reduce dramatically. Multifactor authentication is one of the Essential HPH CPGs and one of the most important security measures to implement in 2024.



Healthcare Security Breaches at HIPAA-Regulated Entities

The HIPAA Breach Notification Rule requires all breaches of protected health information to be reported to OCR and individual notifications to be sent to the affected individuals within 60 days of the discovery of a data breach. When a data breach occurs at a business associate of a HIPAA-covered entity, the entity that reports the breach will be dictated by the terms of the business associate agreement. Business associates often self-report their data breaches to OCR, but their covered entities may choose to report the breach themselves, or a combination of the two. For instance, Maximus Inc. disclosed in an SEC filing that the data of between 8 million and 11 million individuals was compromised in its MOVEit Transfer hacking incident, but Maximus reported the breach to OCR as affecting 2,781,617 individuals. Several clients chose to report the breach themselves.

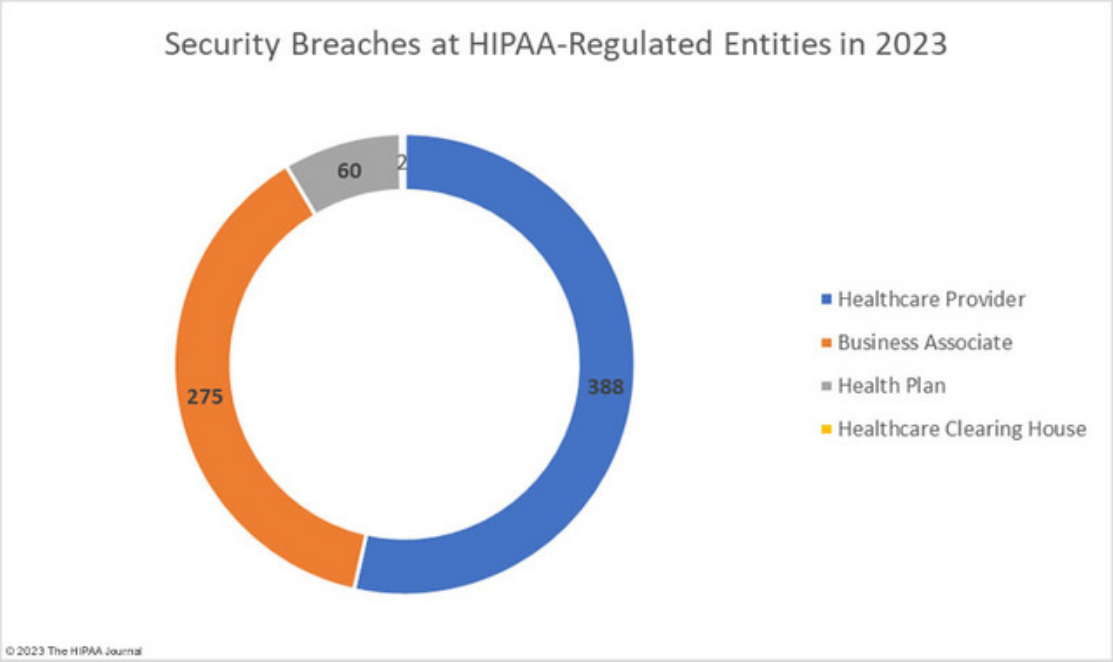
The OCR breach data shows data breaches by the reporting entity, and as such, using that data for analyses means business associate data breaches will be underrepresented. In the table below we show data breaches by reporting entity and the charts reflect where the breach actually occurred.

Healthcare Security Breaches in 2023 – Reporting Entity

Entity Type	Data Breaches	Records Breached
Healthcare Provider	450	39,925,448
Business Associate	170	77,347,471
Health Plan	103	15,792,548
Healthcare Clearinghouse	2	3,075

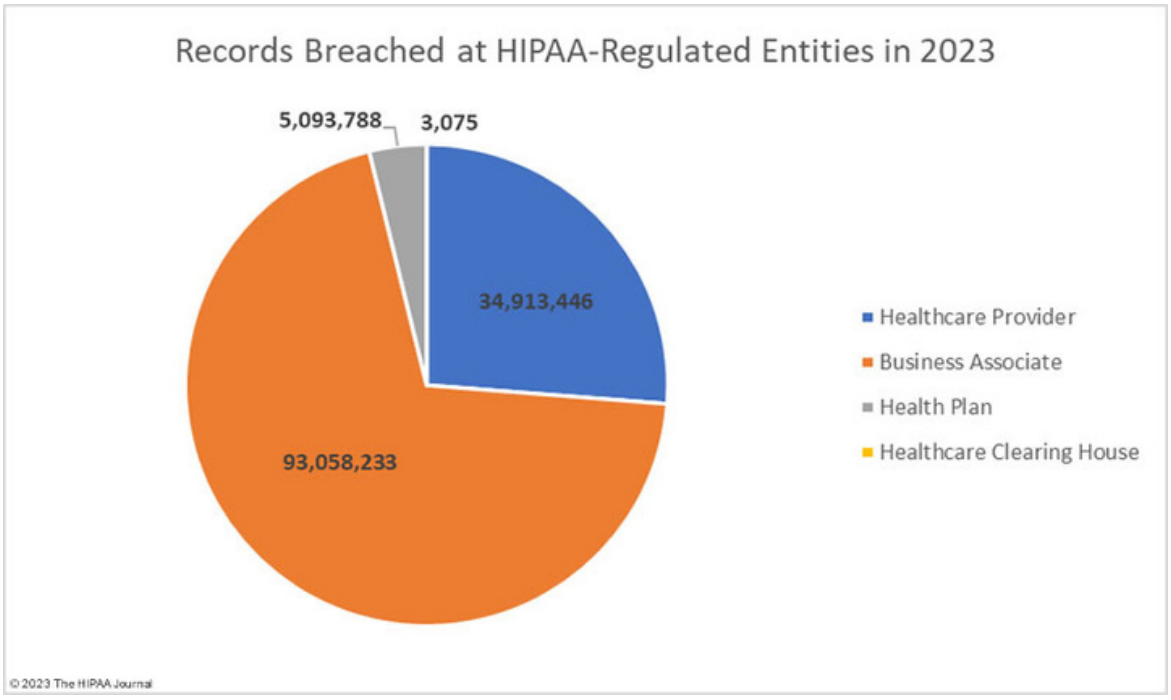
Healthcare Security Breaches in 2023 – Location of Data Breach

The adjusted data shows healthcare providers suffered the most data breaches; however, data breaches at business associates were more severe, with more than 2.5 times as many records breached at business associates than at healthcare providers.



The average size of a data breach at a healthcare provider was 89,983 records (median 5,354 records) whereas the average breach at a business associate was 338,394 records (median 5,314 records). 11 of the top 15 security breaches in healthcare in 2023 occurred at business associates of HIPAA-covered entities.

Securing the supply chain is one of the biggest cybersecurity challenges in healthcare. Healthcare organizations often outsource certain functions to specialist vendors and health systems often rely on dozens, if not hundreds, of different vendors, many of which require access to protected health information and every vendor used introduces risk.



Healthcare organizations need to conduct due diligence on their vendors, including assessing their security controls. Before onboarding any new vendor it must be made abundantly clear what the business associate's responsibilities are with respect to HIPAA, data security, and breach reporting.

Strengthening the security of the supply chain is labor-intensive and costly, and many healthcare organizations lack the appropriate resources to devote to vendor risk management, but vendor risk management failures can have significant ramifications. An inventory should be maintained on all vendors, including details of the business associate agreements, and data provided to each. A risk assessment should be conducted before onboarding any vendor including an assessment of their security posture. If a vendor fails to meet the necessary cybersecurity requirements, then they should not be used.

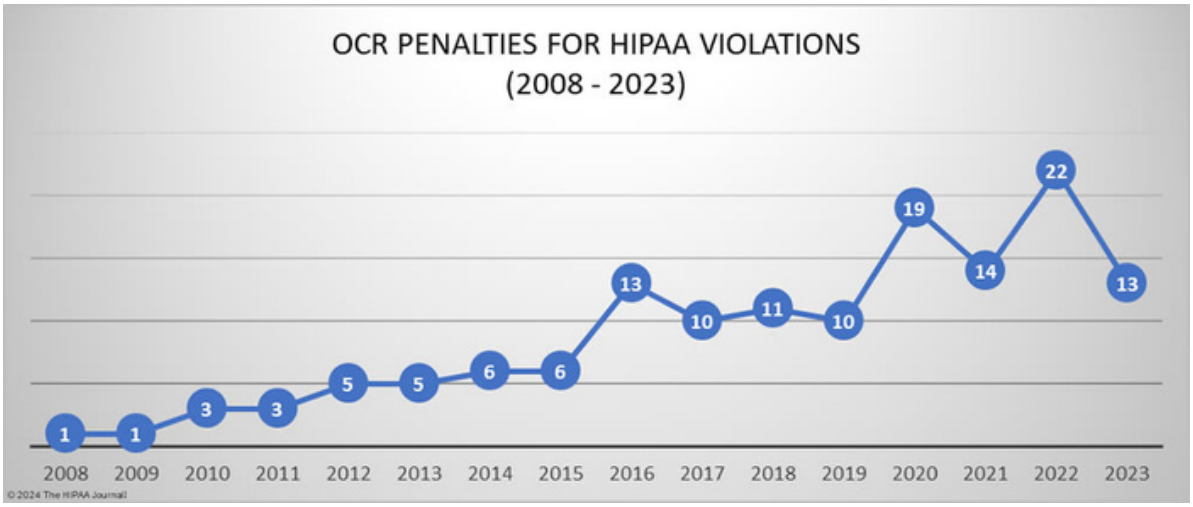
If there is no suitable alternative, then controls should be put in place to manage risk and reduce it to a low and acceptable level. While vendors may confirm that they have implemented reasonable and appropriate safeguards and data security policies and procedures, there are no guarantees that those policies and procedures will be followed and cybersecurity standards maintained. Conducting assessments of vendor security at intake is not sufficient. There should be ongoing reviews and audits of vendors and suppliers. If an organization lacks the personnel to handle this in-house, then third-party consultants should be engaged to assist with these processes. Third-party risk management requirements are included in both the Essential and Enhanced CPGs announced by the HHS in January 2024.

HIPAA Security Breaches Reported in All 50 States

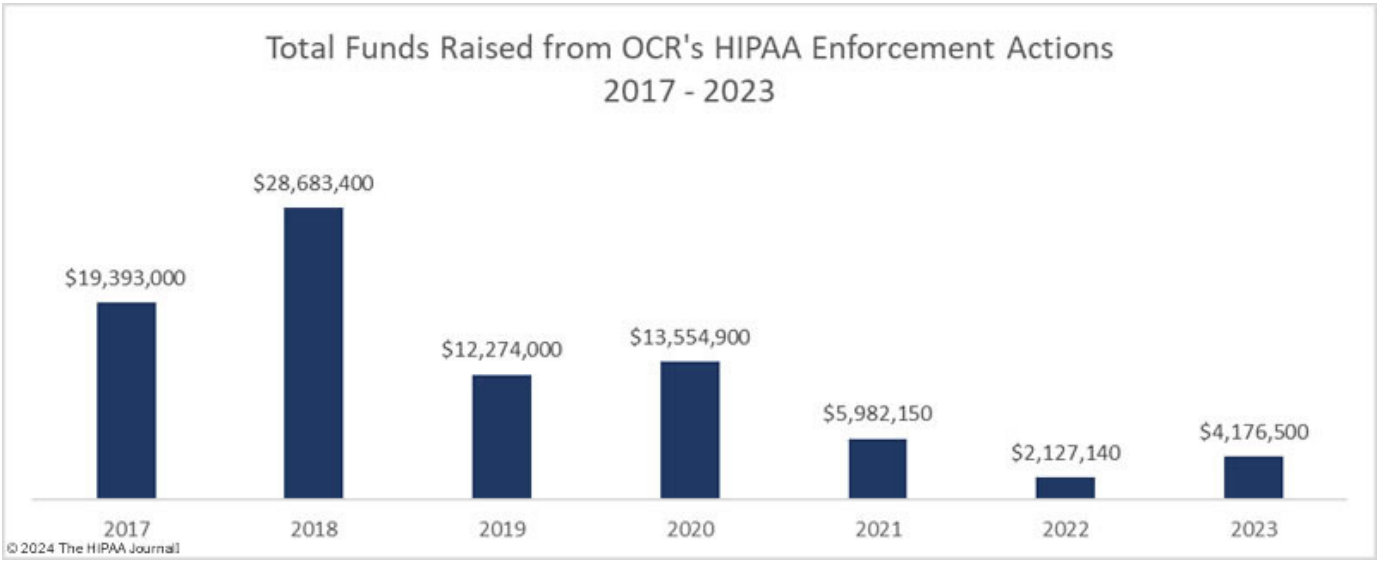
No U.S. state was able to avoid a healthcare security breach in 2023. Data breaches of 500 or more records were reported in all 50 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. The states that experienced the most data breaches are the most heavily populated and have the highest number of HIPAA-regulated entities

Number of Data Breaches			
California	80	Kansas & Oregon	12
New York	63	Washington	11
Texas	58	Kentucky, Missouri, Mississippi & Wisconsin	10
Pennsylvania	40	Colorado	9
Massachusetts	39	Alabama	8
Illinois	36	Utah	7
Florida	33	Arkansas, Oklahoma, and South Carolina	6
Georgia & New Jersey	21	Alaska	5
Arizona & Minnesota	17	Idaho, Louisiana, Maine, North Dakota & West Virginia	4
Connecticut, Maryland, Michigan & Ohio	16	Delaware & New Mexico	3
Indiana, North Carolina & Tennessee	15	Montana, Nebraska, New Hampshire & Nevada	2
Virginia	14	Hawaii, Rhode Island, South Dakota, Vermont, Wyoming	1
Iowa	13	District of Columbia, Puerto Rico & the U.S. Virgin Islands	1

HIPAA Enforcement Activity in 2023



In 2023, OCR announced 13 settlements with HIPAA-regulated entities to resolve allegations of HIPAA violations, a 40.9% reduction from the previous year. These investigations stemmed from reviews of HIPAA compliance in response to reported data breaches and investigations of complaints from patients and health plan members about potential HIPAA violations. While the number of financial penalties fell, the funds raised from OCR enforcement actions increased from $2,124,140 in 2022 to $4,176,500 in 2023.



Since 2019, the majority of penalties imposed by OCR resolved alleged violations of the HIPAA Right of Access. The HIPAA Right of Access requires individuals to be provided with a copy of their health records, on request, within 30 days of that request being received and they should only be charged a reasonable, cost-based fee for exercising that right if they are charged at all.

Since OCR launched its HIPAA Right of Access enforcement initiative in the fall of 2019, 46 penalties have been imposed for HIPAA Right of Access violations, 4 of which were in 2023. This is a significant reduction from the 17 HIPAA Right of Access fines imposed in 2022.

Penalties were imposed for other HIPAA Privacy Rule violations in 2023, including one penalty for a lack of policies and procedures relating to access to PHI by employees and one penalty for the failure to obtain authorization from patients before disclosing their PHI to a reporter.

Following the overturning of the penalty imposed on the University of Texas MD Anderson Cancer Center in 2018, OCR appears to have been reluctant to pursue financial penalties for Security Rule violations in all but the most egregious cases. In 2023, OCR imposed seven penalties to resolve potential violations of the HIPAA Security Rule.

Violations of several HIPAA Security Rule provisions were cited in these enforcement actions, with t6 of the 7 enforcement actions involving risk analysis failures. Another common violation was the failure to maintain and review logs of activity in information systems containing ePHI to identify unauthorized access.

One of the penalties stemmed from a report of snooping on medical records by security guards, with OCR determining there was a failure to implement policies and procedures relating to HIPAA Security Rule compliance and a lack of HIPAA Privacy Rule training.

OCR Enforcement Actions in 2023 Resulting in Financial Penalties

HIPAA-Regulated Entity	Penalty Amount	Penalty Type	Individuals Affected	Reason for Penalty
LA Care Health Plan	$1,300,000	Settlement	1,498	Risk analysis failure, insufficient security measures, insufficient reviews of records of information system activity, insufficient evaluations in response to environmental/operational changes, insufficient recording and examination of activity in information systems, and impermissible disclosure of PHI
Banner Health	$1,250,000	Settlement	2.81 million	Risk analysis failure, lack of reviews of information system activity, lack of verification of identity for access to PHI, and a lack of technical safeguards
Lafourche Medical Group	$480,000	Settlement	34,862	No risk analysis prior to the 2021 phishing incident, and no procedures to regularly review logs of system activity prior to the incident
MedEvolve Inc.	$350,000	Settlement	230,572	Risk analysis failure, lack of a business associate agreement, and an impermissible disclosure of PHI
Yakima Valley Memorial Hospital	$240,000	Settlement	419	Lack of HIPAA Security Rule policies and procedures
Optum Medical Care	$160,000	Settlement	6	Failure to provide individuals with timely access to their medical records
Doctors' Management Services	$100,000	Settlement	206,695	Risk analysis failure, lack of reviews of records of system activity, lack of policies/procedures to comply with the HIPAA Security Rule, and impermissible disclosure of PHI
UnitedHealthcare	$80,000	Settlement	1	Failure to provide an individual with timely access to their medical records
St. Joseph's Medical Center	$80,000	Settlement	3	Disclosure of the PHI of patients to a reporter and a lack of HIPAA Privacy Rule training
iHealth Solutions (Advantum Health)	$75,000	Settlement	267	Risk analysis failure and an impermissible disclosure of PHI
Manasa Health Center, LLC	$30,000	Settlement	4	Impermissible PHI disclosure in response to online review
Life Hope Labs, LLC	$16,500	Settlement	1	Failure to provide an individual with timely access to their medical records
David Mente, MA, LPC	$15,000	Settlement	1	Failure to provide an individual with timely access to their medical records

Attorney General Penalties for HIPAA Violations in 2023

The was a major increase in enforcement actions by state attorneys general in 2023 in response to security breaches in healthcare, with 15 settlements reached with HIPAA-regulated entities to resolve violations of HIPAA and state consumer protection laws. In 2022 there were only three settlements with attorneys general to resolve HIPAA violations, four in 2021, and three in 2019. The majority of the penalties imposed in 2023 by state attorneys general resolved violations of the HIPAA Security Rule that were uncovered during data breach investigations. The majority of these cases involved a lack of reasonable and appropriate security measures such as multifactor authentication, access controls, encryption, security testing, data logging and monitoring, data retention, and up-to-date asset inventories.

Four settlements in 2023 came from multi-state actions. Since the entities concerned operated in multiple states, attorneys general pooled their resources and conducted joint investigations. The largest penalty of the year was imposed on Blackbaud and resolved multiple violations of the HIPAA Security Rule that contributed to a breach of the personal and protected health information of 5.5 million individuals.

State attorneys general in Oregon, New Jersey, Florida & Pennsylvania joined forces in an investigation of a 2.1 million-record data breach at EyeMed Vision Care, and Pennsylvania & Ohio conducted a joint investigation of DNA Diagnostics Center over a 45,600-record data breach, both of which uncovered multiple HIPAA Security Rule failures.

32 states and Puerto Rico participated in an investigation of the Puerto Rican healthcare clearinghouse, practice management software, and electronic medical record provider Inmediata. HIPAA Security Rule failures were identified that led to a breach of the protected health information of more than 1.5 million individuals, followed by violations of the HIPAA Breach Notification Rule.

California imposed a massive penalty on Kaiser Foundation Health Plan Foundation Inc. and Kaiser Foundation Hospitals. The case was resolved for $49 million and related to the improper disposal of PHI and hazardous waste, with the bulk of the settlement amount concerned with the latter.

State Attorney General	HIPAA-Regulated Entity	Penalty Amount	Penalty Type	Individuals Affected	Reason for Penalty
49 States and the District of Columbia	Blackbaud	$49,500,000	Settlement	5,500,000	Failure to implement appropriate safeguards to ensure data security and breach response failures, which violated the HIPAA Security Rule, Breach Notification Rule, and state consumer protection laws
California	Kaiser Foundation Health Plan Foundation Inc. and Kaiser Foundation Hospitals	$49,000,000	Settlement	7,700	Violations of HIPAA for the improper disposal of PHI and violations of several state laws for the improper disposal of hazardous waste
Oregon, New Jersey, Florida & Pennsylvania	EyeMed Vision Care	$2,500,000	Settlement	2.1 million	Lack of administrative, technical, and physical safeguards, and access control failures – use of the same password by several employees.
32 States and Puerto Rico	Inmediata	$1,400,000	Settlement	1,565,338	Failure to implement appropriate safeguards to ensure data security, failure to conduct a secure code review, and data breach notification failures
New York	Practicefirst	$550,000	Settlement	1.2 million	Patch management failure, lack of encryption, and a lack of security testing.
New York	U.S. Radiology Specialists Inc.	$450,000	Settlement	198,260, including 92,540 New York residents	Failure to upgrade hardware to address a known vulnerability
California	Kaiser Permanente	$450,000	Settlement	Up to 167,095 individuals	Mailing error that resulted in an impermissible disclosure of PHI, failure to promptly halt mailings when there was a known error and negligent maintenance or disposal of medical information
New York	Healthplex	$400,000	Settlement	89,955 (62,922 New York residents)	Violation of New York's data security and consumer protection laws (data retention/logging, MFA, data security assessments)
New York	Personal Touch Holding Corp dba Personal Touch Home Care	$350,000	Settlement	753,107 (316,845 New York residents)	Only had an informal information security program, insufficient access controls, no continuous monitoring system, lack of encryption, and inadequate staff training
New York	New York Presbyterian Hospital	$300,000	Settlement	54,396	Violations of the HIPAA Privacy Rule and New York Executive Law due to the use of pixels on its website that transmitted PHI to third parties
Indiana	Schneck Medical Center	$250,000	Settlement	89,707	Failure to address known vulnerabilities in a timely manner and breach notification failures.
New York	Heidell, Pittoni, Murphy & Bach LLP	$200,000	Settlement	61,438 New York residents	Widespread non-compliance with the HIPAA Security Rule – 17 HIPAA violations
Pennsylvania & Ohio	DNA Diagnostics Center	$400,000	Settlement	45,600	Lack of safeguards to detect and prevent unauthorized access, failure to update asset inventory, and disable/remove assets that were not used for business purposes.
Indiana	CarePointe ENT	$125,000	Settlement	48,742	Failure to correct known security issues in a reasonable time frame, lack of business associate agreement
Colorado	Broomfield Skilled Nursing and Rehabilitation Center	$60,000 ($25,000 suspended)	Settlement	677	Violations of HIPAA data encryption requirements, violation of state data protection laws, and deceptive trading practices.

Outlook For 2024

It has been a particularly bad year for security breaches in healthcare with hacking incidents continuing to increase in number as well as severity. Cyber actors will continue to target the healthcare industry and with fewer victims paying ransoms, these attacks may even increase as ransomware actors attempt to maintain their incomes.

In 2023 we saw increasingly aggressive tactics by ransomware groups including swatting attacks on patients when their healthcare provider refused to pay the ransom and these aggressive tactics look set to continue.

To reduce security breaches in healthcare, more must be done than achieving the minimum cybersecurity standards of the HIPAA Security Rule. If all healthcare organizations implemented the recently announced HHS Essential Cybersecurity Goals, there would be a marked reduction in healthcare cybersecurity breaches in 2024.

In practice that will be difficult for many healthcare organizations due to limited budgets and a chronic shortage of skilled cybersecurity professionals; however, the HHS plans to make funding available to help cover the initial cost of security improvements and establish an incentive program for adopting the Enhanced Security Goals.

These measures will go a long way toward raising the baseline level of cybersecurity in the healthcare industry and improving resilience to cyber threats.

Please see updates on this page:

https://www.hipaajournal.com/security-breaches-in-healthcare/