



# 2023 VELOCITY HEALTHCARE DATA BREACH REPORT

An analysis of healthcare data breaches  
from 2009 through 2022

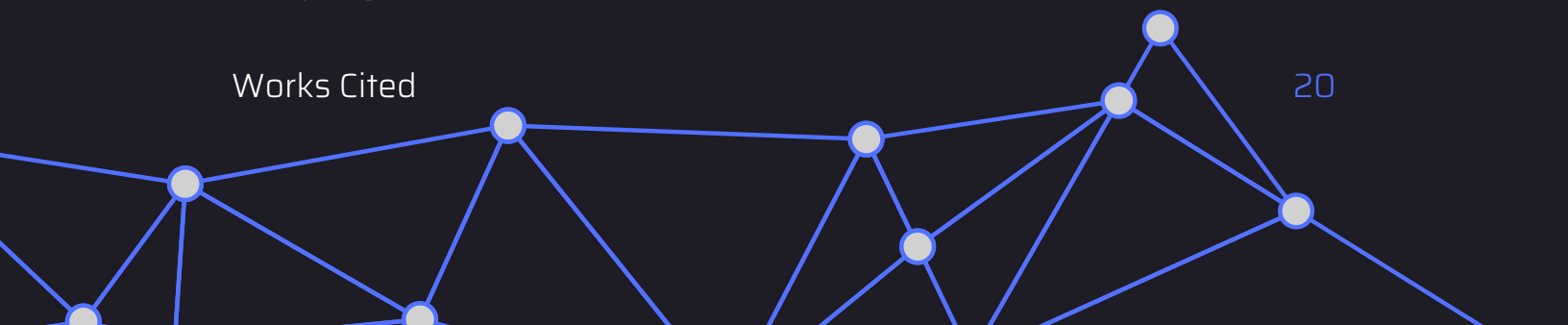
JULY 2023

Prepared by  
Stern Security



# Table of Contents

Background	03
Executive Summary	04
Findings	06
Summary	06
Underreported Records	07
Breach Trends	08
Breach Categories	09
Breach Location	13
Meta Pixel Breaches	14
Third-Party Breaches	16
Good News	17
Conclusion	18
Resources	18
Company	19
Works Cited	20



# Background

## Over 5,000 Healthcare Breaches Analyzed

In its second annual healthcare data breach report, Stern Security has critically analyzed over 5,000 data breaches since the Department of Health and Human Services (HHS) began tracking the information in 2009. Stern Security utilized data from their HealthcareBreaches.com website as well as published information from HHS to create this comprehensive study. Stern Security augmented the HHS data by investigating each breach in 2022 to fully understand the cause of the incident.

This report shows critical insights into healthcare breach trends over the past 13 years. It covers everything from the number of breaches attributed to ransomware to the number attributed to third-parties (business associates). This year, Stern Security has added a new breach categorization - the number of breaches due to analytics software including Meta (Facebook) Pixel. Once again, a new breach record was established with more healthcare breaches occurring in 2022 than any previous year. This report puts forth a detailed analysis.



# Executive Summary

Over time, cyber-attacks have transitioned from minor nuisances to significant threats against the critical infrastructure. The healthcare industry has been particularly hit hard with 5,160 publicly reported breaches occurring from 10/21/2009 through 12/31/2022. Within those breaches, 388,987,820 Protected Health Information (PHI) records were lost. In 2022 alone, there were 719 reported healthcare breaches with 54,434,957 PHI records lost.

---

## 388,987,820

Number of PHI records lost from 10/21/2009 to 12/31/2022

---

While there are various forms of breaches such as physical theft and unauthorized access of a patient record, there is no surprise that hacking is the top threat. In 2022, 78.9% of healthcare breaches and 85.2% of PHI records lost were due to hacking. Within the hacking category, ransomware dominates the news cycle with stories of hospitals needing to revert to paper records or divert patients elsewhere because their systems were unusable. Ransomware was attributed to 24% of all healthcare breaches last year.

Meta (Facebook) made the healthcare security news with a report stating that a number of healthcare organizations were sending patient data to the social networking giant via their Meta Pixel analytics software. Webpage analytics software, including Meta Pixel, is generally used to track user behavior such as page views and button clicks. However, some analytics software may send identifiable information to the parent company. In total, 6,358,104 PHI records were breached due to Meta Pixel in 2022.

Most companies rely on third parties (business associates) for essential functionality and services. Unfortunately, business associates continue to have a significant impact on breaches. In 2022 business associates accounted for 35.3% of the healthcare breaches and 45% of the PHI records lost. On a positive note, third-party breaches, while still high, have flatlined over the past few years.

Long term trend lines point to a continued increase in the rate of healthcare breaches with hacking leading the surge, and ransomware and third-party sources having the greatest impact.



# Findings

## Summary

The United States Department of Health and Human Services (HHS) published its first healthcare breach notification on October 21st, 2009. It must be noted that all of the breaches published by HHS contain 500 or more Protected Health Information (PHI) records lost so the data within this report fit the same criteria.

5,160

Number of healthcare breaches from 10/21/2009 - 12/31/2022

Between 10/21/2009 and 12/31/2022, there were 5,160 healthcare breaches. These breaches caused a loss of 388,987,820 PHI records. To put these numbers in prospective, this has now surpassed the entire US population of 333,287,557 (United States Census Bureau, 2022). Clearly some breached PHI records cross-reference to the same individuals.

54,434,957

HEALTHCARE  
RECORDS  
LOST IN 2022

NUMBER OF  
BREACHED  
HEALTHCARE  
RECORDS  
SURPASSES  
U.S.  
POPULATION

719

HEALTHCARE  
BREACHES IN  
2022

## Underreported Breached PHI Records

The total number of breached PHI records may be far greater than the reported amount.

Healthcare organizations must report within 60 days any breach with over 499 PHI records lost. However, the exact number is often initially underestimated. For example, in one breach notification, a social services provider reported a breach of 1,000 records to HHS, but their later report to a state attorney general's office stated 184,183 records lost (Adler, 2023). The initial 1,000 records reported to HHS may have been a placeholder until the actual number was determined. As of mid-July 2023, the organization has yet to correct their initial admission on the HHS portal.

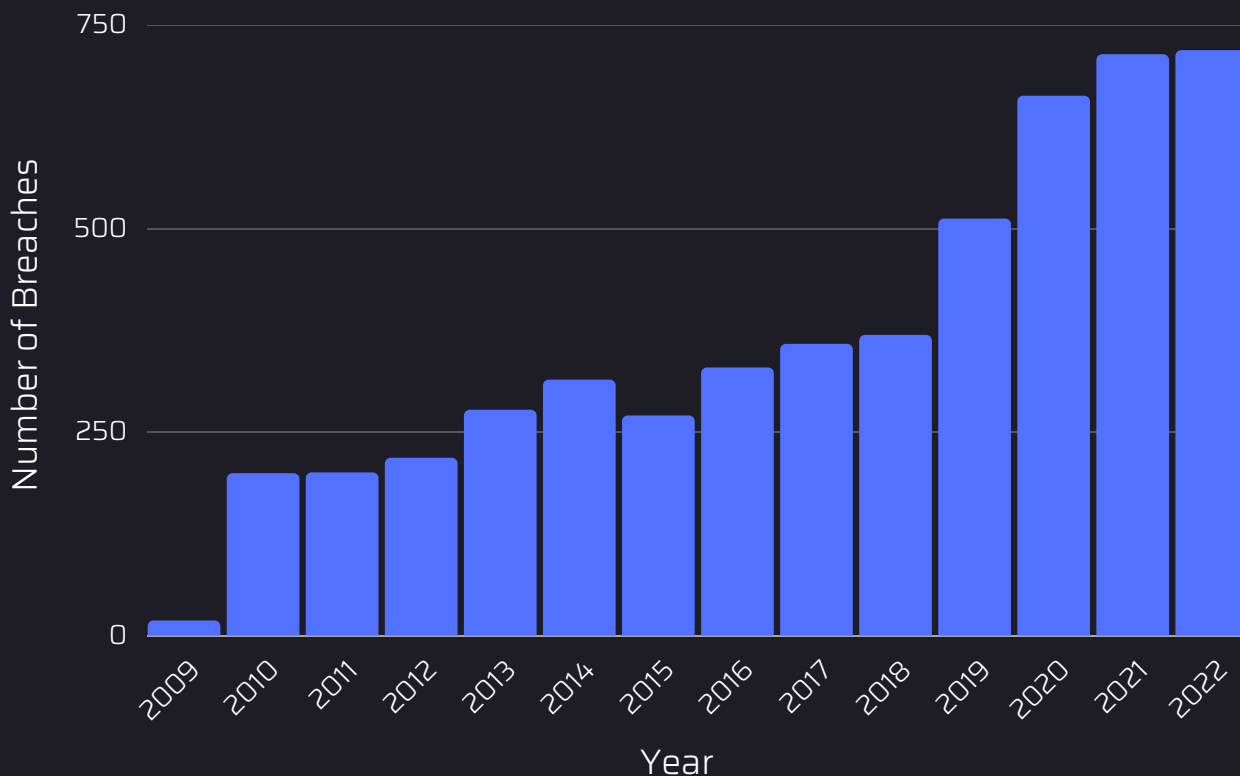


## Breach Trends

From 2010\* to 2022, healthcare breaches climbed almost every year with an average of 43 more breaches per year. While the number of breaches was roughly unchanged from 2021 to 2022, during the past five years there was a 95% total increase in breaches. The 719 breaches in 2022 was the largest number of breaches recorded in a single year.

\*2009 is not included as it was a partial year total.

Number of Healthcare Breaches by Year



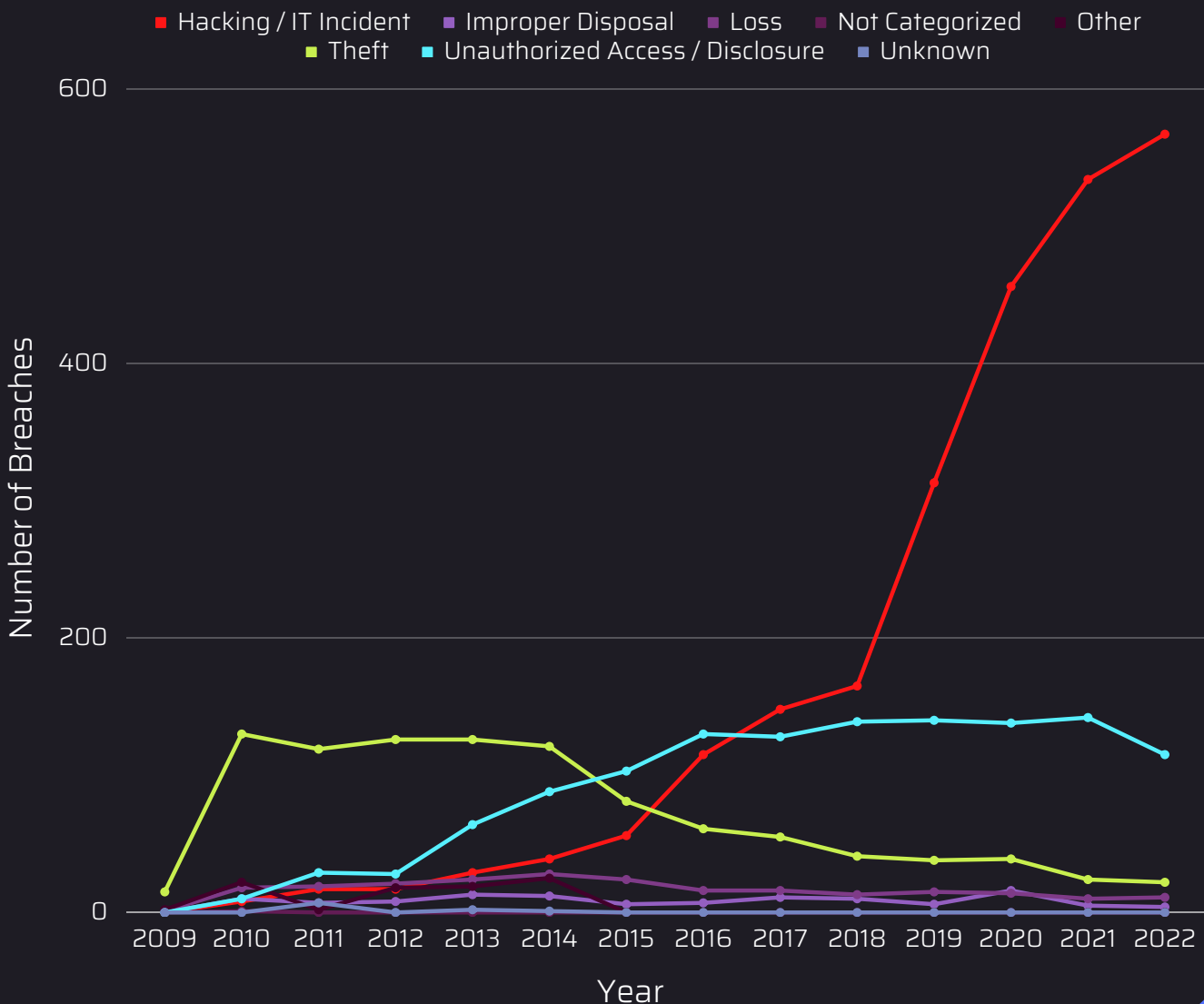




## Breach Categories

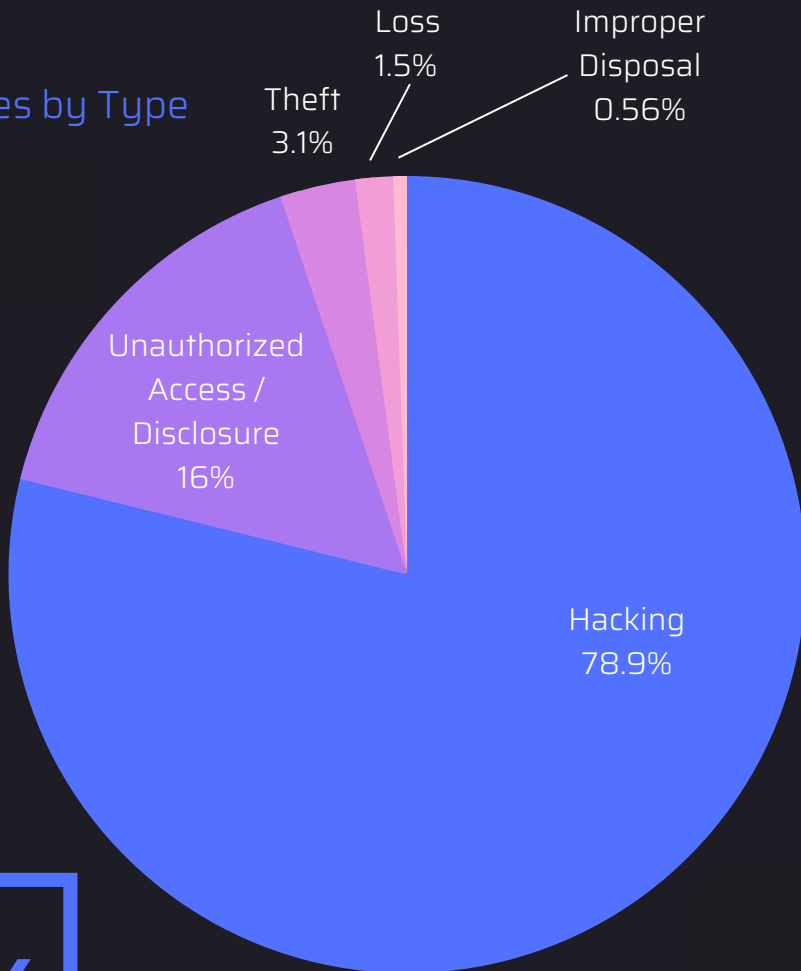
Healthcare breaches are divided into different categories depending on how the breach occurred. The primary categories are Hacking, Theft (physical), and Unauthorized Access/Disclosure. Examples of Unauthorized Access/Disclosure include patient records sent to the incorrect patient, inadvertently published PHI, and healthcare workers accessing data that they were not authorized to do so. While there are multiple sources of data breach, the high breach trend is mostly due to hacking which is clearly visible in the graphs.

Healthcare Breaches by Type



In 2022, 78.9% of healthcare breaches and 85.2% of PHI records lost were due to hacking. The number of breaches due to “Unauthorized Access/Disclosure” came in at a distant second place, but still had a visible impact on breach counts.

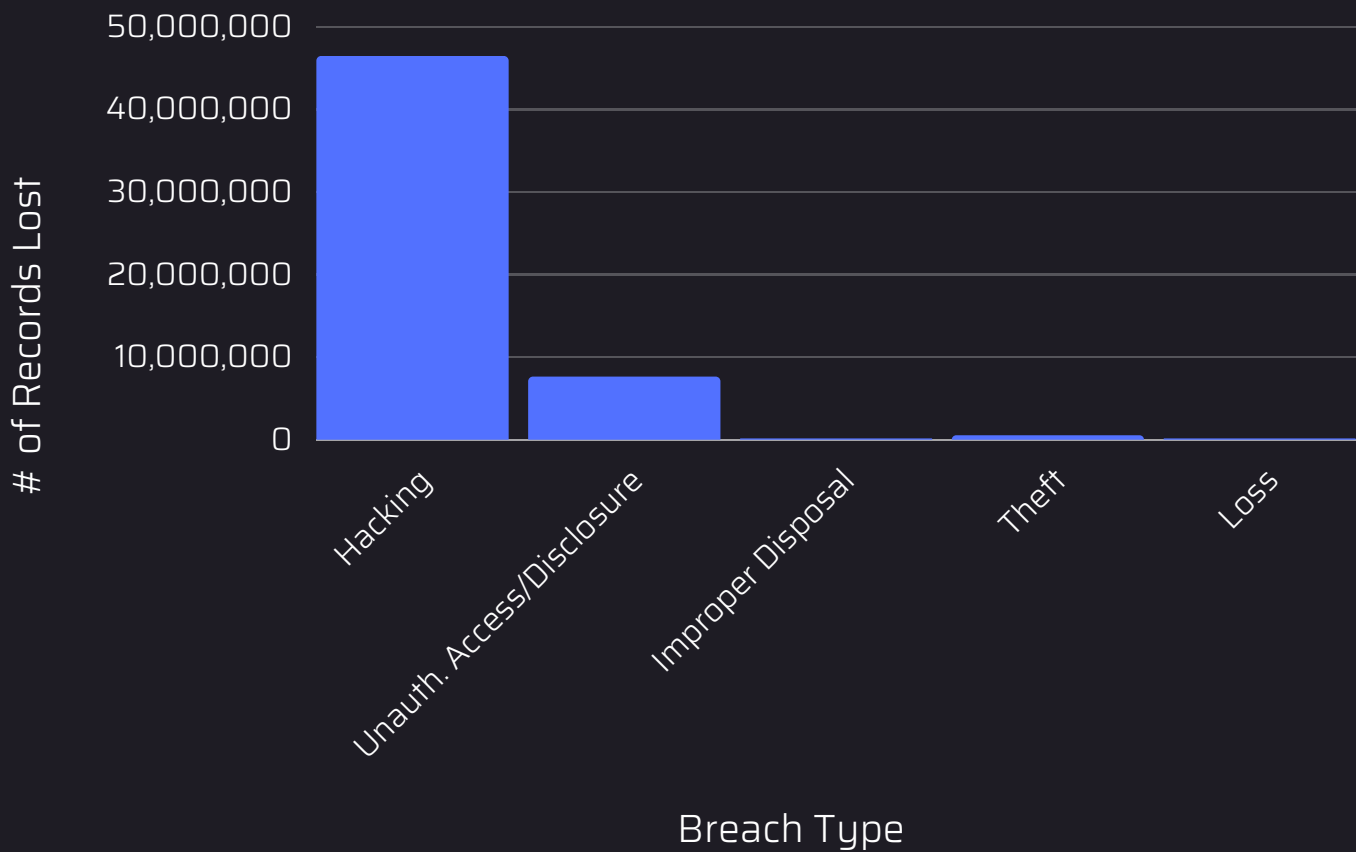
2022 Healthcare Breaches by Type



**78.9%**  
BREACHES  
DUE TO  
HACKING

Not surprising, most of the PHI records lost in 2022 were due to hacking. During the year, 46,382,896 PHI records were lost due to hacking alone. To put in perspective, that roughly corresponds to the PHI records of the entire populations of California and Arizona being hacked.

Number of Protected Health Records Lost in 2022 by Breach Type

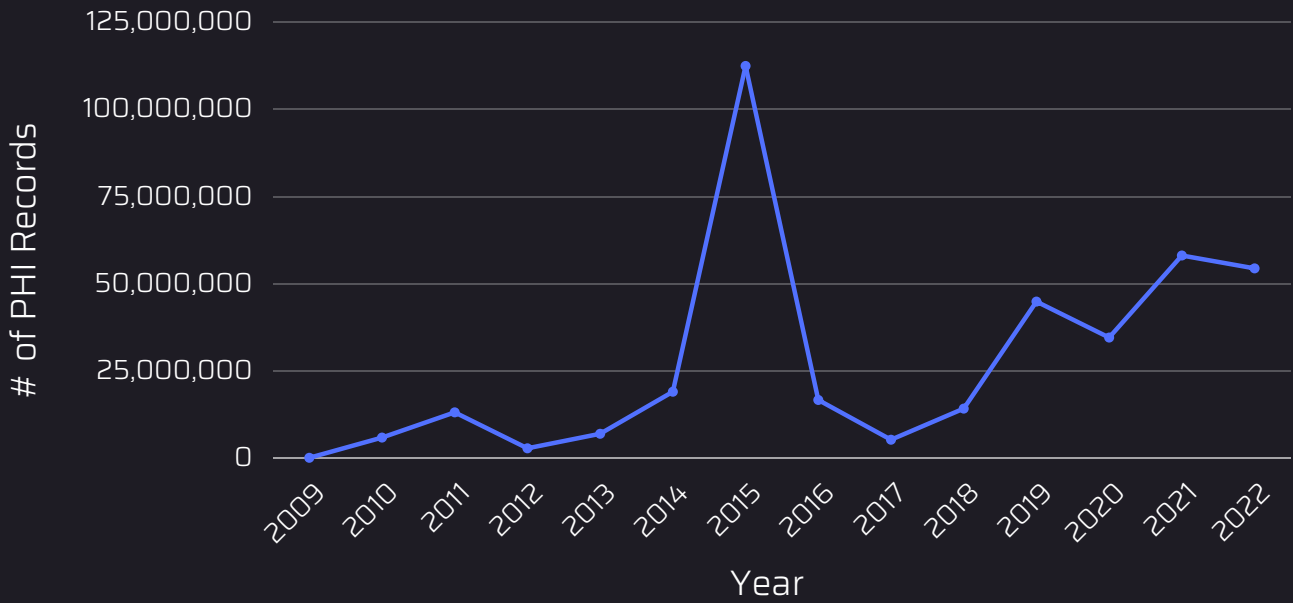


Stern Security researched all of the breaches that occurred in 2022 to gain more insight into how the breaches occurred. Among types of hacking incidents, ransomware remains a dominant threat as **24%** of all healthcare breaches in 2022 were due to ransomware.



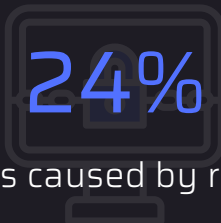
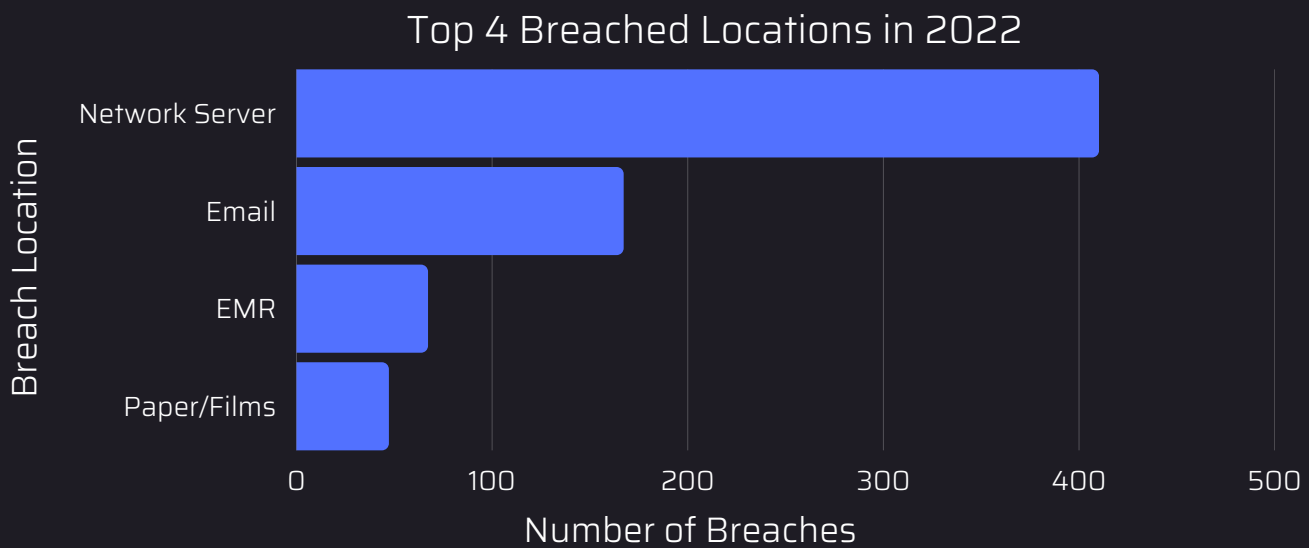
With the exception of a few very large data breaches in 2015, the number of Protected Health Information (PHI) records lost has generally increased over the years. Outside of 2015, the number of PHI records lost has increased at an average of 4,400,000 records per year.

Number of PHI Records Lost over the Years

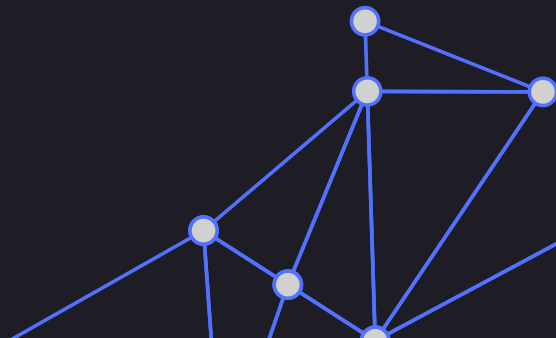


## Breach Location

The Department of Health and Human Services (HHS) tracks the type of system that the breach occurred. The top four sources included Network Server, Email, Electronic Medical Record (EMR), and Paper/Films. It must be noted that some breaches involved multiple device types.



Healthcare breaches caused by ransomware in 2022



## Meta Pixel Breaches

Meta, formally the Facebook company, made headlines as their Meta Pixel analytics software was listed as the source of multiple healthcare breaches. In June of 2022, an article published by The Markup stated that 33 of the top 100 hospitals were sending sensitive data to Facebook via their Meta Pixel web analytics tool (Feathers, Fondrie-Teitler, Waller, & Mattu, 2022). Analytics software on web pages is used to track user behavior. However, some analytics tools send more data than simple button clicks or visitor counts, and could also send text and identifiable information. Additionally, some analytics software could possibly track user behavior across other platforms as well if the information is identifiable. The Department of Health and Human Services (HHS) and the Federal Trade Commission issued a warning to healthcare organizations about the privacy and security risks from online tracking software (U.S. Department of Health and Human Services, 2023).

---

# 6,358,104

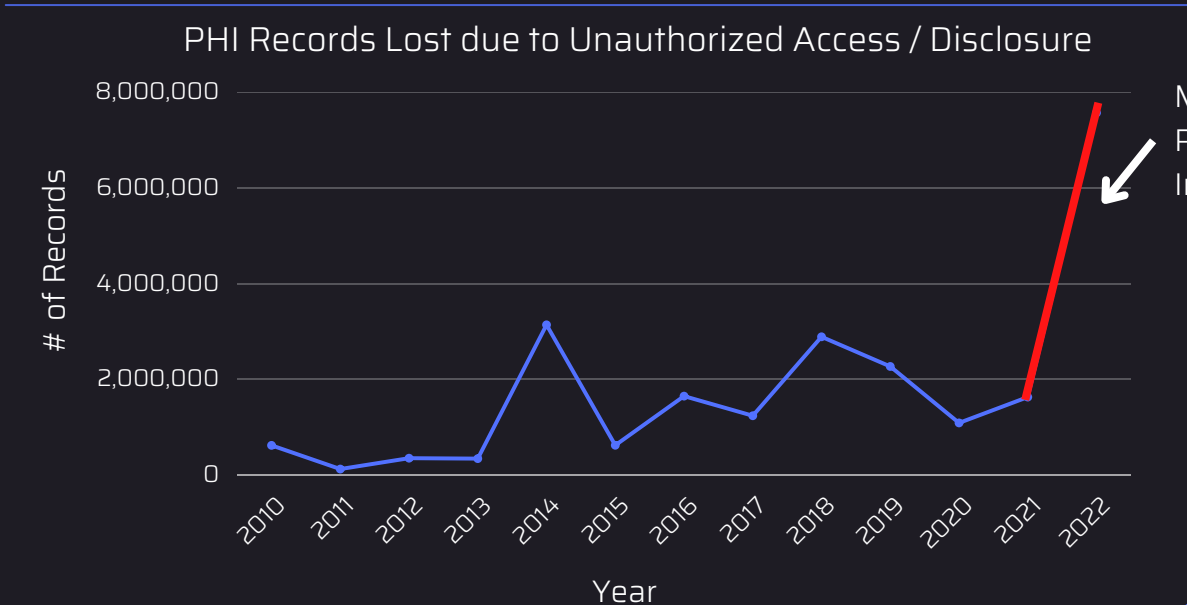
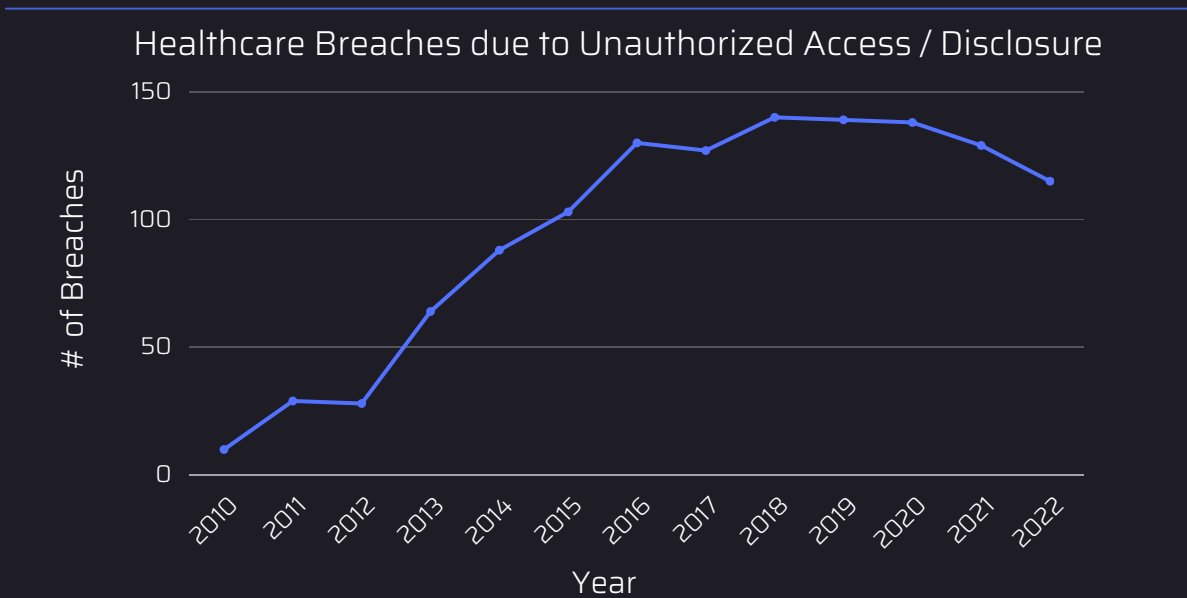
PHI records breached due to Meta Pixel in 2022

---

Multiple hospitals had the Meta Pixel code on the patient scheduling pages while seven hospitals had the analytics software within their password-protected patient portals. In total, 6,358,104 reported patient records were breached due to the Meta Pixel tracker in 2022. These breaches occurred within four hospital systems per the Department of Health and Human Services (HHS). Of the seven hospitals that The Markup listed as having Meta Pixel installed on their patient portal, three (43%) reported a data breach in 2022.

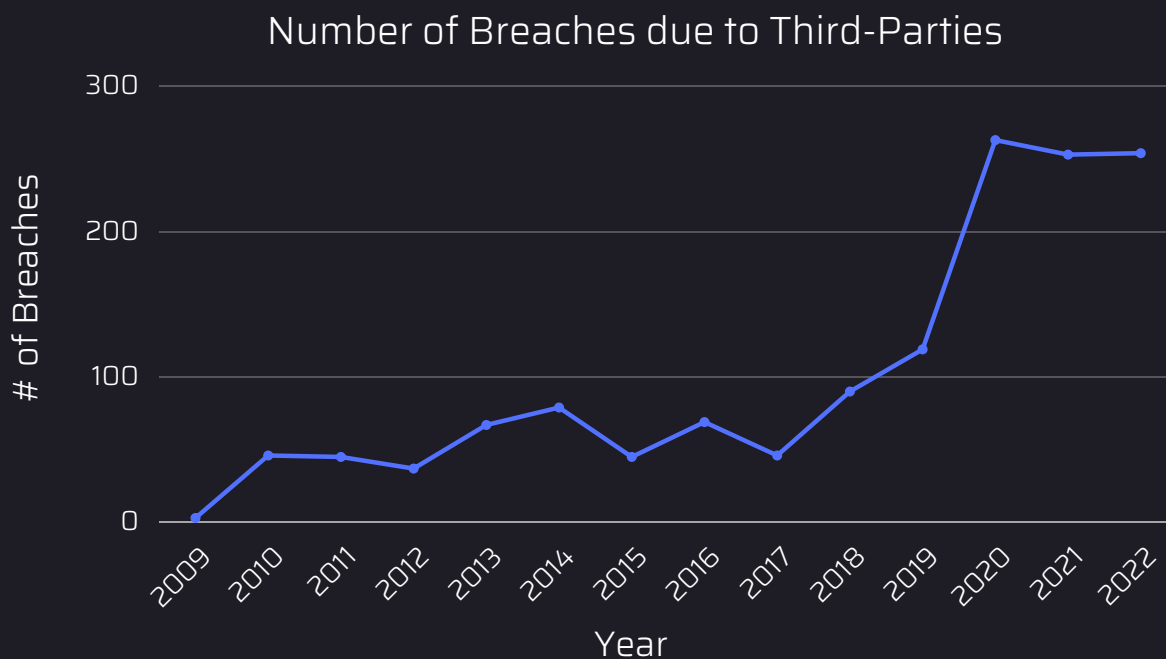


The Meta Pixel and other analytics software breaches in healthcare are far from over as several hospitals have already listed breaches due to this in 2023. These breaches will appear in next year’s report. It is important to note that while breaches due to unauthorized access decreased in 2022, the patient records lost in 2022 increased dramatically. With over 6,000,000 PHI records lost due to Facebook, these divergent trends are clearly the result of breaches from Meta Pixel.



## Third-Party Breaches

Third-parties, referred to as “Business Associates” in healthcare, have had a significant impact on breaches. In 2022, while third-parties were responsible for 35.3% of the healthcare breaches, they were responsible for 45% of the records lost. Although healthcare breaches due to third-parties leveled off during 2020-2022, from 2010 to 2019 they were on an exponential growth pattern, with an average growth rate of 14% per year. From 2019 through 2022, PHI records lost due to third-party breaches averaged 24,800,000 records per year.



45%

PHI records breached due to 3rd parties in 2022

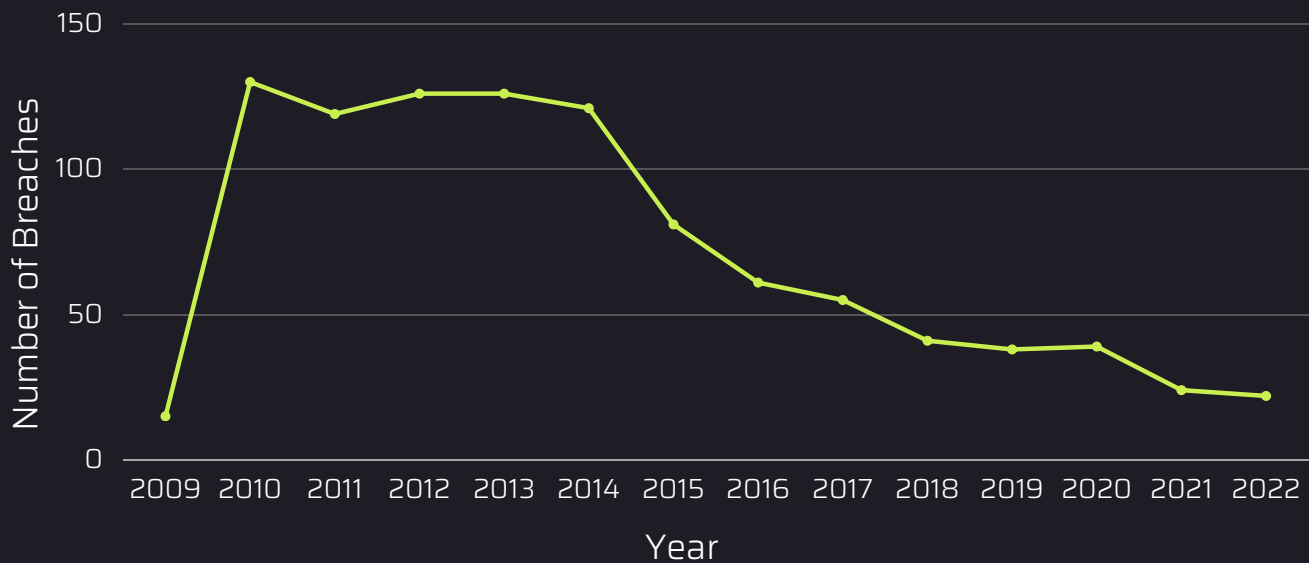


## Good News

While healthcare breaches and PHI records lost remain a serious concern which must be addressed, there is some good news:

1. **Decline of PHI Records Lost in 2022** - The number of patient records lost in 2022 declined slightly from 2021.
2. **Third-Party Breach Flatline** - The number of breaches due to third-parties has flatlined over the last few years
3. **Physical Theft Decline** - Breaches due to physical theft have been on a steady decline. Examples include stolen laptops and filing cabinets that contain PHI. This decline could be because of an increased use of full disk encryption on devices combined with less use of paper records.

Number of Healthcare Breaches due to Theft



## Good Breach News

Healthcare Breaches due to **theft** have been on a **steady decline**.



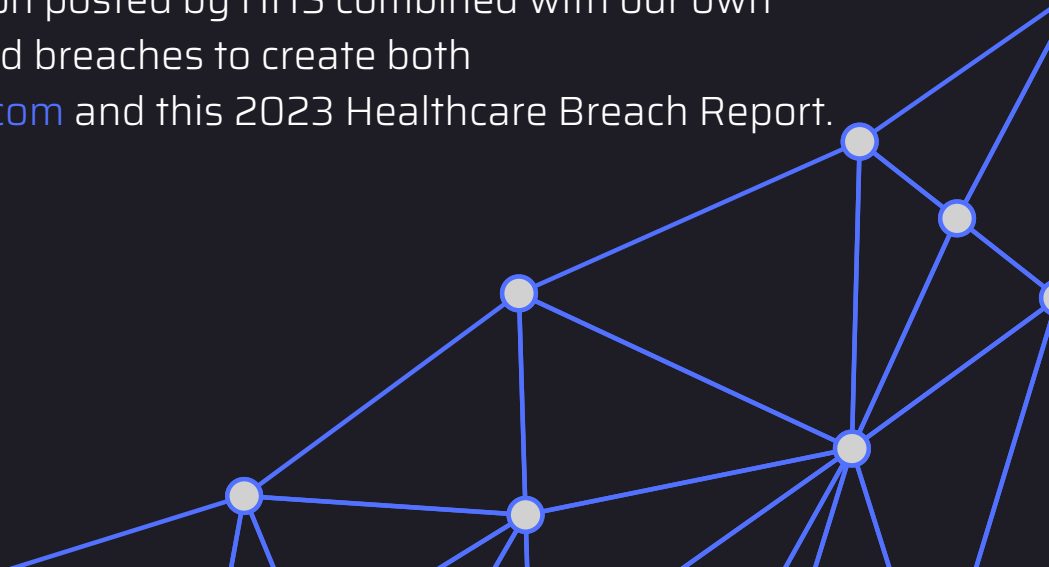
# Conclusion

The trends point to a continued increase in the rate of healthcare breaches each year with hacking leading the surge. Ransomware continues to have a large impact on healthcare breaches. Breaches due to third-parties (business associates) also continue to have a large impact on breach trends. Analytics programs such as Meta Pixel will continue to be a growing source of healthcare breaches in 2023.

On a positive note, some trends are going in the right direction such as the steady drop over the years in the number of breaches due to physical theft. Also, healthcare breaches due to third-parties has flatlined over the past few years. We must learn from these incidents in order to guard this incredibly sensitive PHI, flatten the breach curve, and secure the planet.

# Resources

Health and Human Services (HHS) publicly posts a list of breaches of Protected Health Information (PHI) affecting 500 or more individuals per section 13402(3)(4) of the HITECH Act. Stern Security utilized the information posted by HHS combined with our own research into the listed breaches to create both [HealthcareBreaches.com](https://www.healthcarebreaches.com) and this 2023 Healthcare Breach Report.





# Company

Stern Security is a leading cybersecurity company and the creator of the [HealthcareBreaches.com](https://www.healthcarebreaches.com) Executive Dashboard.

Stern Security developed [Velocity \(https://www.velocitysec.com\)](https://www.velocitysec.com), the innovative cybersecurity insights SaaS platform. Based on the most accurate internal and third-party risk assessment information, [Velocity](https://www.velocitysec.com) creates actionable plans to help organizations prioritize risk and increase security posture. Try Velocity for free today.

Stern Security's services division conducts comprehensive [penetration testing](#), threat emulation, analytics software integration security reviews, and Virtual CISO (Chief Information Security Officer) engagements. "Secure the Planet" is Stern Security's motto and we believe that everyone can play a role.

If you appreciated the report and would like to hear more about our products and services (or just want to say thank you), contact us!


Contact form: <https://www.sternsecurity.com/contact/>

 LinkedIn: <https://www.linkedin.com/company/sternsecurity>

 Twitter: [https://twitter.com/stern\\_security](https://twitter.com/stern_security)

 Instagram: <https://www.instagram.com/sternsec/>

 Vimeo: <https://vimeo.com/sternsecurity>

 Facebook: <https://www.facebook.com/sternsec>

Velocity Cybersecurity Insights Platform:  
<https://www.velocitysec.com/>



# Works Cited

Adler, S. (2023, January 27). Up to 184,000 Clients of Lutheran Social Services of Illinois Impacted by Ransomware Attack. Retrieved from The HIPAA Journal: <https://www.hipaajournal.com/up-to-184000-clients-of-lutheran-social-services-of-illinois-impacted-by-ransomware-attack/>

Feathers, T., Fondrie-Teitler, S., Waller, A., & Mattu, S. (2022, June 16). Facebook Is Receiving Sensitive Medical Information from Hospital Websites. Retrieved from The Markup: <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>

U.S. Department of Health & Human Services. (2022, March 30). U.S. Department of Health and Human Services Office for Civil Rights. Retrieved from Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information : [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)

U.S. Department of Health and Human Services. (2023, July 20). HHS Office for Civil Rights and the Federal Trade Commission Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies. Retrieved from U.S. Department of Health and Human Services: <https://www.hhs.gov/about/news/2023/07/20/hhs-office-civil-rights-federal-trade-commission-warn-hospital-systems-telehealth-providers-privacy-security-risks-online-tracking-technologies.html>

United States Census Bureau. (2022, July 1). U.S. and World Population Clock. Retrieved from United States Census Bureau: <https://www.census.gov/popclock/>

