WHITE PAPER

Analyzing the cost per record of healthcare data breaches

Jessica Payne, Senior Consultant, Healthcare
SECURITY+ | CYSA+ | CC | CCSA | CHPS

CALFIRE ADVISORY

Table of Contents

Introduction		**Page 02**
The value of medical records on the black market		**Page 03**
Healthcare cybersecurity regulatory frameworks: the role of HIPAA and the HHS	Overview of HIPAA Role of HHS	**Page 03**
Cost per record for healthcare organizations	Organizational costs Comparison with other industries	**Page 05**
Data breach trends and projections		**Page 06**
Action steps for mitigating the risk of breaches	Administrative safeguards Physical safeguards Technical safeguards	**Page 06**
Conclusion		**Page 06**

Introduction

Data breaches have emerged as a prevalent threat in today's interconnected digital environment, impacting organizations across various sectors. However, the healthcare industry is particularly vulnerable, facing greater financial repercussions per compromised record. As healthcare organizations increasingly digitize records to enhance patient care and streamline operations, they inadvertently expose themselves to substantial cybersecurity risks. According to the 2024 Verizon Data Breach Investigations Report, healthcare organizations represented 11% of all U.S. data breaches in 2024. Such frequency increases the importance for healthcare organizations to understand the financial implications associated with these incidents.

This white paper investigates the cost per record associated with healthcare breaches, detailing the organizational costs involved and the value of stolen healthcare information on the black market.

The value of medical records on the black market

Hackers target medical records because they are more valuable than other types of personal data, such as credit card information, which typically sells for much less. On the black market, the cost of medical records is notably high, reflecting their value to cybercriminals. According to a recent analysis by Keeper, the cost of medical records on the black market (over $1,000 each) starkly contrasts with the value of personal information from other industries. For instance, credit card details typically fetch only $5 to $20, while login credentials for online accounts may sell for $1 to $10. This staggering price difference is due to the wealth of sensitive information that medical records contain, including personal identification details, medical histories, and insurance information. The increased market value of healthcare data can also be attributed to several factors:

- **Use in fraudulent activities:** Stolen healthcare information is highly valuable for identity theft, filing false insurance claims, and obtaining medical services fraudulently. This propensity for misuse drives demand and, consequently, market prices.
- **Scarcity of healthcare data:** The unique and sensitive nature of healthcare records makes them more desirable than other data types, enhancing their market value. Criminal organizations actively seek this data to facilitate a wide range of illicit activities.
- **Impact on victims:** The long-term consequences of healthcare data breaches can be devastating for individuals, leading to identity theft, compromised medical care, and significant emotional distress, further amplifying the perceived value of such information on the black market.

Medical records can be used for identity theft, fraud, and various forms of financial exploitation. Further, medical record information is not only useful for immediate financial gain but can also be exploited over a longer period. As the demand for such sensitive information persists, the black market for medical records continues to thrive, posing significant risks to individuals and healthcare institutions alike.

Given the attractiveness of medical records for cybercriminals, how do healthcare organizations protect themselves? And what are the costs if they don't?

Healthcare cybersecurity regulatory frameworks: the role of HIPAA and the HHS

Overview of HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 established national standards for the protection of health information. The HIPAA Privacy Rule and HIPAA Security Rule set forth requirements for the safeguarding of protected health information (PHI):

- **HIPAA Privacy Rule:** Governs how healthcare providers, health plans, and other entities handle PHI, including who can access this information and under what circumstances. It establishes patients' rights regarding their health information, including the right to receive notice of breaches.
- **HIPAA Security Rule:** This rule outlines the security requirements for electronic PHI (ePHI), mandating that organizations implement administrative, physical, and technical safeguards to protect against data breaches.

HIPAA regulations are essential in maintaining the confidentiality and security of healthcare data and provide a framework that healthcare organizations must follow. Failure to comply with HIPAA can result in severe penalties, with fines reaching up to $1.5 million per violation category per year.

Role of HHS

The U.S. Department of Health and Human Services (HHS) plays a critical role in enforcing HIPAA regulations. The Office for Civil Rights (OCR) within HHS is responsible for investigating complaints and conducting compliance reviews related to HIPAA violations. The OCR has the authority to impose civil monetary penalties and ensure that organizations take corrective actions following a breach.

According to the 2024 HIPAA Accomplishments and Wrap-Up by HHS, OCR was very active with HIPAA enforcement throughout 2024. OCR completed 22 HIPAA enforcement actions (the second highest in OCR history) and collected over $9.9 million in settlements and civil money penalties. Issues resolved included violations related to ransomware, phishing, health information left unsecured on the internet, impermissible access to ePHI, reproductive health information impermissibly disclosed, and untimely patient access to PHI.

Any calculation of the economic impact of data breaches within the healthcare sector must, therefore, include the financial burden of regulatory fines in combination with the costs related to the required corrective actions.

Cost per record for healthcare organizations

Organizational costs

The financial impact of a data breach for healthcare organizations is multifaceted, encompassing various key components that generally fall into the two categories of direct and indirect costs:

- **Direct costs:** Immediate expenses arising from a data breach include the cost of breach notifications, forensic investigations, legal fees, and regulatory fines. For instance, a healthcare provider may incur costs related to notifying affected patients, engaging cybersecurity firms to investigate the breach, and addressing any legal ramifications.
- **Indirect costs:** Indirect costs often surpass direct expenses and can significantly affect the long-term financial health of the organization. These costs may include reputational damage, loss of patient trust, increased insurance premiums, and potential business loss due to operational disruptions.

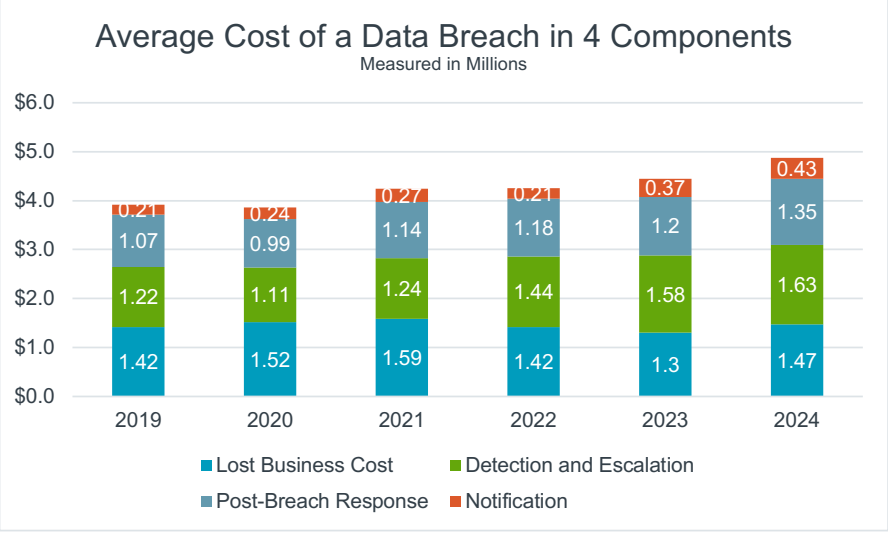


Figure 1: Cost of a data breach per component

According to the 2024 IBM Cost of a Data Breach Report, the average total cost of a healthcare data breach reached approximately **$9.7 million** (Figure 2), compared to an overall average cost of **$4.88 million**, with an average cost per medical record escalating to **$500+**. This figure marks a notable increase over the previous year's reported cost and remains significantly higher than the average cost per record in other industries, which stands at around **$10-100+**.

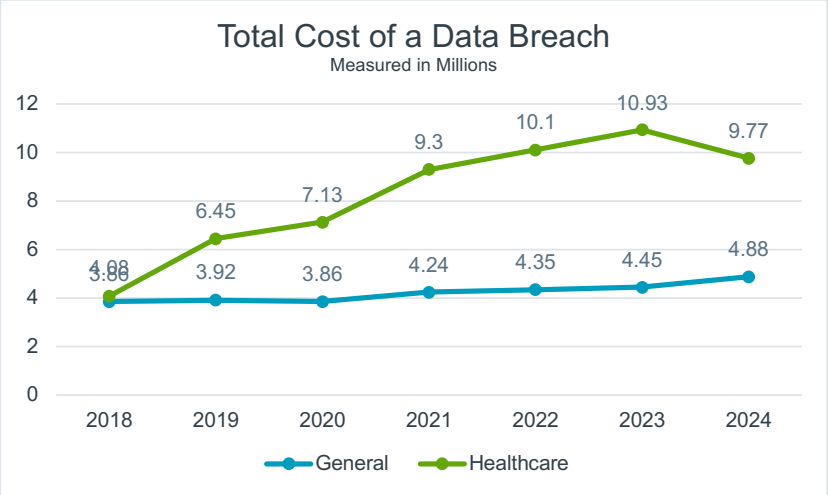


Figure 2: Total cost of a data breach - healthcare vs general by year

Comparison with other industries

The healthcare industry has with notably higher average costs associated with data breaches. As stated above, recent data from IBM (Figure 3) states that healthcare incurs an average cost (**$9.77 million**) per breach far surpassing the costs faced by other industries.

For context, the financial services sector averages around **$6.08 million**, while technology firms experience costs averaging **$5.45 million**. Other industries, including public services, retail, and education have significantly lower average costs, ranging from approximately **$2.55 million** to **$4.09 million**.

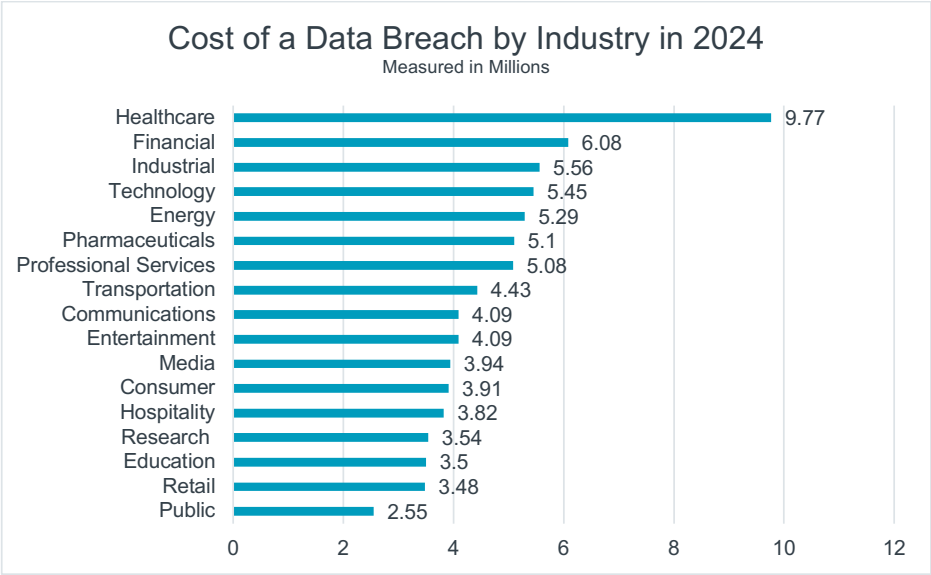


Figure 3: Total cost of a data breach - healthcare vs general by industry

This stark contrast underscores the unique vulnerabilities and regulatory challenges faced by healthcare organizations, which must safeguard highly sensitive patient information while navigating stringent compliance requirements such as HIPAA and other frameworks.

Several factors contribute to the disparity in breach costs between healthcare and other sectors:

- **Regulatory compliance:** Healthcare organizations are subject to stringent regulations such as HIPAA, which necessitates significant investment in security infrastructure and legal counsel, leading to higher overall costs.
- **Sensitive nature of data:** Healthcare records contain highly sensitive personal information, including medical histories, Social Security numbers, and insurance details. This sensitivity increases both the impact of breaches on patients and the costs associated with remediation.
- **Complexity of healthcare systems:** The intricate nature of healthcare systems, characterized by numerous interconnected entities and technologies, creates multiple potential points of vulnerability. This complexity complicates security efforts and raises costs.

The heightened financial impact of data breaches in healthcare not only affects organizational bottom lines but also threatens patient trust and the integrity of the healthcare system. As such, understanding these costs and the factors driving them is critical for healthcare leaders seeking to bolster their cybersecurity posture and protect their valuable data assets.

Data breach trends and projections

Ransomware is projected to escalate significantly in 2025, as attackers continue to evolve their strategies by targeting critical suppliers that entire industries depend on. The impactful 2024 attacks on CDK Global and Change Healthcare highlighted the extensive disruption caused when a single supplier is compromised, affecting automotive services and healthcare providers nationwide. As a result, there is an urgent need for comprehensive risk analysis within the healthcare industry.

Key trends include:

- **Increased ransomware attacks:** Ransomware attacks on healthcare organizations have risen sharply, indicating that 67% of healthcare breaches involved ransomware in 2024, a significant increase from previous year of 60%, according to Sophos. These attacks not only disrupt operations but also drives up costs as organizations must address the immediate threat while also managing the fallout.
- **Greater regulatory scrutiny:** As data breaches continue to rise, regulators are likely to impose stricter compliance measures on healthcare organizations. The potential for increased fines and sanctions will further elevate the costs associated with data breaches.

Action steps for mitigating the risk of breaches

To mitigate the risk of data breaches and ensure compliance with HIPAA regulations, Coalfire recommends that healthcare organizations implement the following administrative, physical, and technical safeguards:

Administrative safeguards

- **Risk assessment:** Conduct regular risk assessments to identify vulnerabilities and areas for improvement in the organization's data protection practices.
- **Training and awareness:** Provide comprehensive training for employees on HIPAA compliance, data privacy, and security protocols. Regular training updates can reinforce the importance of safeguarding PHI.
- **Policies and procedures:** Develop and maintain clear policies and procedures regarding the handling of PHI. Ensure these are communicated effectively to all staff.
- **Incident response plan:** Establish and regularly test an incident response plan that outlines the steps to be taken in the event of a data breach, ensuring that all employees know their roles and responsibilities.

Physical safeguards

- **Access controls:** Implement physical access controls to restrict unauthorized personnel from entering areas where PHI is stored or processed. This may include locked doors, security badges, and visitor logs.
- **Secure storage:** Ensure that physical records are stored securely, such as in locked cabinets or rooms. For electronic devices containing PHI, use secure locations to minimize risk.
- **Device management:** Maintain a policy for the secure disposal of old hardware and electronic devices that may contain PHI, ensuring that data is irretrievably erased before disposal.

Technical safeguards

- **Data encryption:** Use encryption for ePHI both in transit and at rest to protect data from unauthorized access.
- **Access controls:** Implement strong access control measures, such as unique user IDs, passwords, and multi-factor authentication, to limit access to sensitive data.
- **Regular audits:** Conduct regular audits of information systems to ensure compliance with HIPAA regulations and to identify potential vulnerabilities.
- **Patch management:** Keep software and systems up to date with the latest security patches and updates to protect against known vulnerabilities.

Conclusion

The cost per record for healthcare data breaches remains markedly higher than in other industries, driven by both organizational costs and the substantial black-market value of stolen information. As healthcare organizations increasingly rely on digital systems to manage sensitive patient data, the risks and costs associated with data breaches are only predicted to grow. Stakeholders within the healthcare sector must prioritize investments in advanced cybersecurity measures and compliance strategies to effectively mitigate these risks.

By implementing comprehensive administrative, physical, and technical safeguards, healthcare organizations can enhance their compliance with HIPAA and significantly reduce the likelihood of data breaches. Understanding the financial implications of data breaches and the evolving landscape of cyber threats is crucial for healthcare organizations to better prepare for and respond to potential breaches. Enhanced compliance with HIPAA and proactive engagement with HHS can further protect organizations against the financial and reputational damage associated with data breaches, ultimately safeguarding the welfare of patients.

Appendix: Acronyms

Acronym	Term
ePHI	Electronic protected health information
HHS	U.S. Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
OCR	Office for Civil Rights
PHI	Protected health information

Legal Disclaimer

This white paper is provided by Coalfire Systems, Inc. or its subsidiaries ("Coalfire") for informational purposes only. This white paper is the property of Coalfire and is protected by U.S. and international copyright laws. Unauthorized use, reproduction, or distribution of this white paper, in whole or in part, is strictly prohibited. Factual information included in this white paper has been taken from sources that Coalfire believes to be reliable, but its accuracy, completeness, or interpretation cannot be guaranteed. Information is current as of the date of this white paper only and is subject to change without notice. This white paper is provided "as-is" with no warranties, including any warranty of merchantability, fitness for a particular purpose, and non-infringement. Coalfire expressly disclaims all liability arising from or relating to the use of any information or material included in this white paper for any purpose, including any actions taken or not taken based on the contents of this white paper. You are solely responsible for making your own independent assessment of the information in this white paper and for the development, implementation, and execution of your information security program. For questions regarding any legal or compliance matters referenced in this white paper, you should consult your legal counsel, security advisor, or the relevant standard authority.

Concerned about the long-term cost of a breach? Ask us

Between forensic investigations, legal fees, and the erosion of patient trust, the true cost of a breach can be staggering. We'll help you strengthen your security posture to avoid the financial and reputational fallout that follows a cyberattack.

About the Author

Jessica Payne, Senior Consultant, Healthcare

Jessica Payne, BS in Management Information Systems with a focus on Information Assurance, is a certified cybersecurity professional holding CompTIA Security+, CompTIA CySA+, ISC2 Certified in Cybersecurity (CC), Certified in Healthcare Privacy and Security (CHPS), and Certified Cyber Security Architect (CCSA) credentials. Since joining Coalfire in 2024, she has brought over five years of cybersecurity consulting experience, specializing in healthcare risk management and compliance. Jessica works closely with healthcare clients to strengthen their security postures using industry frameworks such as NIST 800 53, NIST CSF, HIPAA, and ISO 27001.

Her expertise includes conducting comprehensive security assessments, developing tailored cybersecurity programs, and ensuring regulatory compliance for healthcare organizations. Jessica has led initiatives in incident response, vulnerability management, and policy development, helping clients mitigate risks and safeguard sensitive data. Dedicated to ongoing professional growth, she stays at the forefront of cybersecurity trends to provide innovative, effective solutions that address evolving security challenges.

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit Coalfire.com.

Copyright © 2026 Coalfire. All rights reserved. The information in this document is subject to change at any time based on revisions to applicable regulations and standards. Any forward looking statements are not predictions and are subject to change without notice. Coalfire is not responsible for any errors or omissions.