Microsoft

Healthcare organizations—strengthen cybersecurity and compliance in the era of AI

Introduction

Today, leaders in the healthcare and life sciences industry face significant pressure to streamline clinical and operational workflows, reduce administrative overhead, and enhance organizational efficiency. They recognize the potential of artificial intelligence (AI) to assist in these endeavors.

At the same time, the evolving threat landscape in the industry makes it imperative for these organizations to strengthen security to help mitigate potential risks.

As a trusted leader, Microsoft understands both the opportunities and risks associated with AI. We can assist healthcare and life sciences organizations to accelerate AI innovation using a secure-by-design digital strategy that enhances compliance, cybersecurity, and patient care.

This document explores industry trends and challenges while providing actionable steps and resources to help organizations prioritize security in an AI environment, mitigate its risks, and maximize its benefits.

Use of AI can lead to concerns about:

- Bias
- Protecting patient data
- Accuracy and reliability
- Explainability
- Patient safety
- Data privacy and regulatory compliance

As noted in a 2023 UK Department for Science, Innovation, and Technology paper, "Pro-Innovation Approach to AI Regulation":

> It is crucial that we do all we can to create the right environment to harness the benefits of AI and remain at the forefront of technological developments. That includes getting regulation right so that innovators can thrive, and the risks posed by AI can be addressed.

Table of contents

An often targeted and heavily regulated industry with patient outcomes at stake

The healthcare industry faces a rapidly increasing range of cybersecurity threats, with ransomware attacks emerging as one of the most significant.

A combination of valuable patient data, interconnected medical devices, and small Security Operations Center (SOC) teams make many healthcare organizations prime targets for threat actors. As healthcare operations become increasingly digitized, from electronic health records (EHR) to telemedicine platforms—the attack surface of hospitals grows more complex and vulnerable.

- 92% of healthcare organizations surveyed experienced at least one cyberattack in the past 12 months.[1]
- According to a recent report from the financial risk advisory firm Kroll, healthcare is now the primary target for cybercriminals.[2]
- Ransomware attacks are costly with healthcare organizations losing an average of $900,000 per day on downtime alone.[3]

Different healthcare industry sectors face unique risks, but the impacts of cyberattacks are similar: They are costly, disruptive, and jeopardize patient safety and protecting against these threats burdens understaffed and overworked SOC teams.

Healthcare is an attractive target for cybercriminals

- Reputation for paying ransoms
- Limited security resources and investments
- Legacy systems and infrastructure vulnerabilities
- Expanding attack surface

Healthcare Cybersecurity: Data Breach Impact

$4.88M

The global average cost of a data breach in 2024. A 10% increase over last year and the highest total ever.[4]

60%

of healthcare organizations were attacked with ransomware in 2023.[5]

$9.77M

was the average cost of a healthcare data breach in 2024, which fell by **10.6%** that year. Despite the drop, healthcare retained its status as the costliest industry for data breaches for the 14th year in a row.[6]

An estimated **190 million** individuals were affected by 14 data breaches involving more than 1 million healthcare records in 2024.[7]

Common concerns facing healthcare industry verticals

Providers
Ransomware, third-party risks

Payors and insurers
Data breaches, third-party risks

Pharmaceuticals
IP theft, supply chain disruption

Recommended reading

Ransomware in healthcare: Key insights from Microsoft's new report | Blog

US Healthcare at risk: Strengthening resiliency against ransomware attacks

Sharing how Microsoft protects against ransomware | Blog

Microsoft to help rural hospitals defend against rising cybersecurity attacks | Stories

Building a more secure future

AI in healthcare provides opportunities to improve patient experiences, streamline operations, and automate administrative tasks. However, it also introduces risks such as data privacy concerns, bias, and evolving regulatory standards for transparency, safety, and accountability. Balancing these factors is essential. Addressing these opportunities and risks requires integrated technology solutions, strong governance frameworks, and compliance with changing mandates.

AI transformation requires a strong cybersecurity foundation. That's why we are focused on helping customers use and build AI that is safe and secure. In the healthcare industry, this involves supporting organizations in protecting patient privacy, meeting regulatory obligations, managing information risk, and maintaining high levels of data security to responsibly adopt AI.

Microsoft Security: empowering healthcare with robust protection

In the rapidly evolving landscape of healthcare, the security of patient data and healthcare systems is paramount. Microsoft Security offers a portfolio of AI-powered, end-to-end security solutions to help healthcare organizations manage security operations across complex IT environments without missing a security alert.

Microsoft helps you leverage AI and automation to assess and strengthen your compliance posture against regulations, manage response incidents, implement controls to govern usage and comply with both regulatory and corporate policies. These solutions are natively integrated into the business applications you use every day and provide the productivity benefits of AI while remaining compliant and secure.

Recommended reading

Read the latest updates from Microsoft Security

Microsoft and HITRUST:

Working with key industry partners on streamlining compliance

With extensive experience working with regulatory bodies in the healthcare industry, we can help accelerate compliance, adoption, and time to value of solutions. One of these partners is the Health Information Trust Alliance (HITRUST). Not only does Microsoft partner with HITRUST, Microsoft is one of the first hyperscale cloud service providers to receive certification for the HITRUST Common Security Framework (CSF), and is certified at the highest HITRUST r2 level of assurance including a broad range of platforms and services across the Microsoft Cloud.[9]

HITRUST created and maintains the HITRUST CSF, a certifiable framework to help healthcare organizations and their providers demonstrate their security and compliance in a consistent and streamlined manner. HITRUST provides a benchmark using a standardized compliance framework, assessment, and certification process against which cloud service providers, third-party business associates and data processors, and covered health entities and data controllers can measure compliance.

In stark contrast with healthcare industry averages, the breach rate of Health Information Trust Alliance (HITRUST)-certified environments in 2022 and 2023 was **0.6%** (99.4% reported no breach), which is drastically lower than healthcare industry averages.[8]

Recommended reading

AI Governance: ISO 42001

AI Security: HITRUST AI Security Assessment and Certification

AI Risk Management: HITRUST AI Risk Management Assessment, NIST AI RMF, ISO 23894

Customer use case

St. Luke's University Health Network prescribes proactive, unified protection with Microsoft Security solutions

Protecting patient data is key to delivering great care at St. Luke's University Health Network. After deploying various security technologies, it was clear that St. Luke's current technology stack was not providing what it needed. St. Luke's needed a security partner to quickly take its complex data and provide a complete picture. St. Luke's turned to Microsoft Security solutions to gain greater visibility into the data it needs to maintain security. Deploying Microsoft Sentinel, Microsoft Defender for Cloud, and Microsoft Defender for Office 365 provided St. Luke's IT team with many benefits, including a holistic view of its data that could be analyzed and presented to decision-makers.

> I believe that Microsoft is likely the first company on the cusp of creating the predictive model that will take us past threat detection and enable threat prevention. That's why we trust Microsoft."
>
> – David Finkelstein
> Chief Information Security Officer
> St. Luke's University Health Network

Read the story here

Customer use case

Steward

Steward Health Care protects patient data in an evolving cyber pandemic through Microsoft Security solutions

Steward Health Care has multiple hospitals across the US and more than 43,000 staff, making its IT security infrastructure complex. During the COVID-19 pandemic, the complexity grew, as did cybersecurity attacks. The hospital sought out solution providers that could improve Steward Health Care defense quality through constant innovation. Offering consistency, innovation, and stability, Steward Health Care moved forward with the Microsoft Security solutions deployed by partner BlueVoyant. After deploying Microsoft Defender for Endpoint, Steward Health Care has seen vast improvements, including expansion into endpoint configuration, firewall management, and data loss prevention.

> “Malicious actors have shown that they too can use machine learning and the most modern cloud technologies. Phishing and ransomware increased by about 600 percent... And if COVID-19 taught us anything, it’s that strategic outsourcing and optimizing vendor relationships is vital.”
>
> – Esmond Kane
> Chief Information Security Officer
> Steward Health Care

Read the story here

Prioritizing security

Microsoft's unique, expansive, and global vantage point gives us unprecedented insight into key trends in cybersecurity. With customers and partners that span across governments, large and small enterprises, consumers, and gamers, we understand the critical nature of security and its potential impact—whether on individual citizens or entire nations.

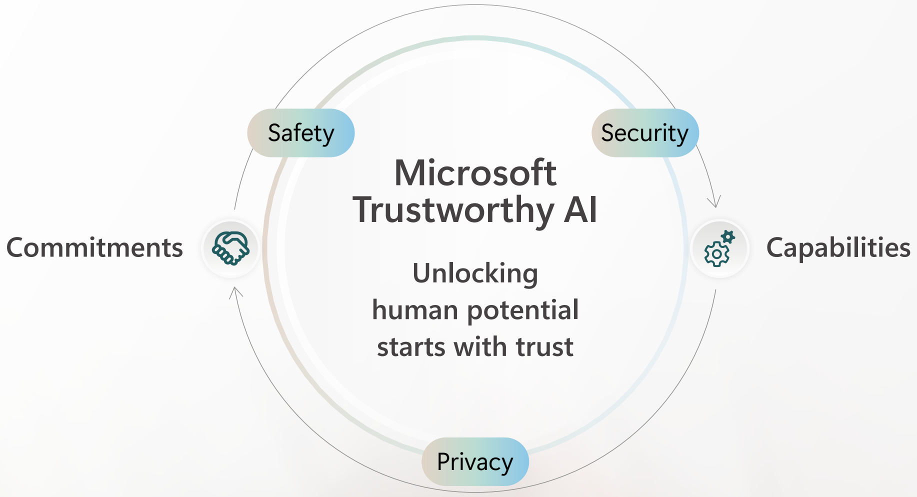
Microsoft has prioritized security above all else and is guided by three principles: secure by design, secure by default, and secure operations.

Our expanded Secure Future Initiative (SFI) underscores the company-wide commitments and the responsibility we feel to make our customers more secure.

As the potential for AI advances, we will continue to focus on helping customers use and build AI that is **secure, safe, and private.**

Our presence in the digital ecosystem[10]

- More than 50 years, serving billions of customers globally
- 78 trillion security signals per day inform our insights
- More than 1,500 unique threat groups tracked
- 34,000 full-time equivalent engineers working on security
- 15,000 partners with specialized security expertise



Start your security and compliance journey with Microsoft AI-powered solutions

Microsoft has been a leader for years in developing AI technologies in accordance with responsible AI principles designed to meet compliance requirements, protect data and systems, and maintain customer trust.

Discover how Microsoft's trusted cloud services, integrated security solutions, AI-powered Copilot for Security, and comprehensive global compliance portfolio and partner network can help healthcare organizations effectively implement AI, manage its risks, and optimize patient outcomes.

Learn more about how AI can help fortify healthcare security and compliance.

Download the infographic →

Additional resources

[Microsoft Security | Secure Our World—Together]

[Microsoft Security | Accelerate AI transformation with strong security]

Sources:

1. Proofpoint. (2024). Ponemon Healthcare Cybersecurity Report.
2. The HIPPA Journal. (February 2025). Healthcare was the most breached industry in 2024.
3. Comparitech. (March 2024). "On average, healthcare organizations lose $900,000 per day to downtime from ransomware attacks".
4. IBM. Cost of a Data Breach Report 2024.
5. Sophos. (September 2024). Two-Thirds of Healthcare Organizations Hit by Ransomware – A Four-Year High, Sophos Survey Finds.
6. TechTarget. (July 2024) Average cost of a healthcare data breach sits at $9.77M. [CB4].
7. Alder, Steve. (January 2025). The Biggest Healthcare Data Breaches of 2024. HIPAA Journal.
8. HITRUST. 2024 Trust Report.
9. Microsoft Learn. HITRUST – Azure Compliance | Microsoft Learn.
10. Microsoft. (2024). Microsoft Digital Defense Report 2024.

Microsoft