

A red rectangular banner with the text 'Healthcare Industry Spotlight' in white, sans-serif font, positioned in the middle left of the image.

Healthcare Industry Spotlight

The main title is written in a large, bold, white, sans-serif font across the bottom half of the image. It is overlaid on a dark, semi-transparent diagonal shape that cuts across the image from the top left to the bottom right. The background of the entire image is a blurred photograph of a healthcare professional in blue scrubs with a stethoscope, working at a desk with a laptop. Floating around the laptop are several white, semi-transparent icons representing medical records, checklists, and data documents.

Global Privacy, AI, and Data Governance for Resilience and Trust

Privacy and Data Governance in Healthcare: What the Industry Needs To Know

Personal health information (PHI) is among the most sensitive data an organization can hold. Details about preexisting medical conditions, treatment plans, payment information, and other data points that can identify individuals are critical for healthcare organizations to effectively administer services. But those qualities also make PHI a high-value target for threat actors and a risk for healthcare organizations that fail to properly secure it.

As one of the most targeted sectors for ransomware and data breaches, healthcare organizations must be aware of the data privacy and governance risks they face, as well as how artificial intelligence is compounding those risks.



Key Challenges Facing Healthcare



Cybersecurity and PHI Protection Remain a Top Priority

According to the [FBI's 2025 Internet Crime Report](#), healthcare ranks as the most targeted sector for ransomware and third most targeted for data breaches. The consequences of a data breach or ransomware attack are immense, with the potential to cause financial damage to healthcare institutions and patients alike. Additionally — and of greater concern — the consequences of these events can cause patient safety risks by preventing providers from administering care because of delayed access to information and disabled equipment.

Cyber Threats to Critical Infrastructure in 2025

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the U.S., their incapacitation or destruction would have a debilitating effect on national security, economic security, or public health and safety.

Sector	Data Breach	Ransomware
Food	~7	0
Water	~9	0
Emergency Services	17	24
Information Technology	21	25
Chemical Industrial Base	9	34
Communications	32	51
Energy	25	54
Commercial	6	59
Transportation	82	83
Health and Healthcare	63	85
Commercial Facilities	84	104
Government Facilities	196	222
Financial Services	174	223
Critical Manufacturing	190	254
Materials & Hazardous Waste	62	328
Healthcare & Public Health	112	400



Regulators Are Increasingly Going Beyond Policy

Written policies and incident response plans alone were once enough to satisfy regulators that an organization was prepared for a cyber incident — but those days are gone. Healthcare regulators and enforcement agencies increasingly expect organizations to demonstrate operational preparedness through activities such as tabletop exercises, network segmentation, access-permission discipline, and rapid detection and isolation capability.

Demonstrating resilience and response capabilities has become increasingly important in mitigating cybersecurity and privacy incidents. When cybercriminals gain unauthorized access to a system, they can lurk inside it for weeks or even months before acting, which makes early detection of a breach essential to reducing the damage incurred.



Third-Party Risk Continues To Be a Focus

Outsourcing a function does not outsource its risk. Healthcare organizations must conduct proper due diligence when contracting with third-party vendors to verify that they are also in compliance with privacy regulations and best practices. Privacy issues resulting from third-party vendors ultimately fall back on the healthcare organization, making due diligence an ongoing process and not simply a one-time exercise approach to risk and an awareness of AI trends can help to prepare organizations for current obligations and future challenges.



AI Risks Are Evolving Rapidly

Like so many other industries, healthcare is leveraging AI's incredible potential to deliver enhanced patient care and operational capabilities. But to function properly, AI tools require data, which for healthcare organizations often means personal information. To safeguard data and meet regulatory standards, organizations must establish effective controls rooted in the principles of transparency and explainability, meaning they understand what data AI has access to and how it's making decisions using that information. Furthermore, healthcare organizations need to verify that a purpose of use exists for the data.





Designing Processes With Privacy in Mind

Privacy and security should be embedded into healthcare technology, services, and products from their inception rather than being added after the fact. By taking a proactive approach to privacy, healthcare organizations can establish a series of actions that prepare their employees for how to handle privacy as opposed to simply looking at what missteps to avoid.



Balancing Functionality and Privacy

Integrated healthcare platforms can provide patients with greater convenience and care options, allowing their information to move among different providers. That convenience isn't without risk, though. When personal information can freely move across a range of networks, providers, and systems, access controls can become challenging. Healthcare organizations must find a balance between the benefits patients receive through shareable information and the importance of privacy considerations and compliance obligations. As new platforms and technology break down silos that once restricted data movement across networks and platforms, real-time monitoring and enhanced visibility into who can access personal data have become a significant priority.

The Need for Training Is as Important as Ever

Privacy and security incidents aren't just caused by external cyberthreats and system control issues. Inappropriate and unauthorized access, whether intentional or not, by those within healthcare organizations presents risks as well. Organizations should focus on continuous training for their employees while keeping an eye on emerging technology and tools that they may need to integrate into those sessions.

Organizations also need to be aware that enforcement bodies are using the same advanced analytics tools as the industries they monitor, enabling enhanced audits and anomaly detection. The regulatory landscape is evolving to keep pace with these advances as well, firmly placing a spotlight on the healthcare industry's compliance with new privacy, security, and AI-related regulatory requirements.



Build Trust Through Stronger Privacy, AI, and Data Governance

BDO's [Global Privacy, AI, and Data Governance for Resilience and Trust](#) e-book looks at how leaders can build operational, trackable governance frameworks that support innovation while reducing regulatory, reputational, and business risk.

BDO's [Privacy & Data Protection Services](#) help organizations develop and implement a comprehensive privacy and data protection strategy to maintain global compliance and responsibly handle personal information.

Explore the **Global Privacy, AI, and Data Governance for Resilience and Trust** e-book ►



Have questions or want to learn more? Contact us!

At BDO, our purpose is to be the people you count on to grow with confidence and achieve what matters most. Our professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization. We are proud to be an ESOP company, inspiring an ownership mindset that enables our collective success.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.

© 2026 BDO USA, P.C. All rights reserved.

