

WHITE PAPER



Managing risks and opportunities that emerging AI technologies present for healthcare cybersecurity



The pitfalls and opportunities that health systems need to know



How do we measure the value and dangers of a new technology? Can an innovation be broadly characterized as beneficial or harmful? The distinction depends far more on the intent behind specific applications than the inherent characteristics of a device, program, or tool. Digital technology in the healthcare industry offers perhaps the most pronounced example of this nuanced spectrum. High-tech medical devices and IT solutions have contributed to life-saving advancements in diagnostics and therapeutics.

The advances in Artificial Intelligence (AI) are some of the most attention-grabbing innovations in recent history. The limit of potential AI applications has yet to be fully discovered and seems to expand continuously. This level of speculation has fueled an incredible amount of attention, excitement, and debate. AI adoption is increasing in the healthcare industry, with particular attention being paid to how AI can help overcome obstacles to diagnostic accuracy and operational efficiency. Yet, as with all digital technology, there is a pressing need for healthcare organizations to proactively manage the cybersecurity risks that AI brings, ensuring patient safety and privacy are protected.

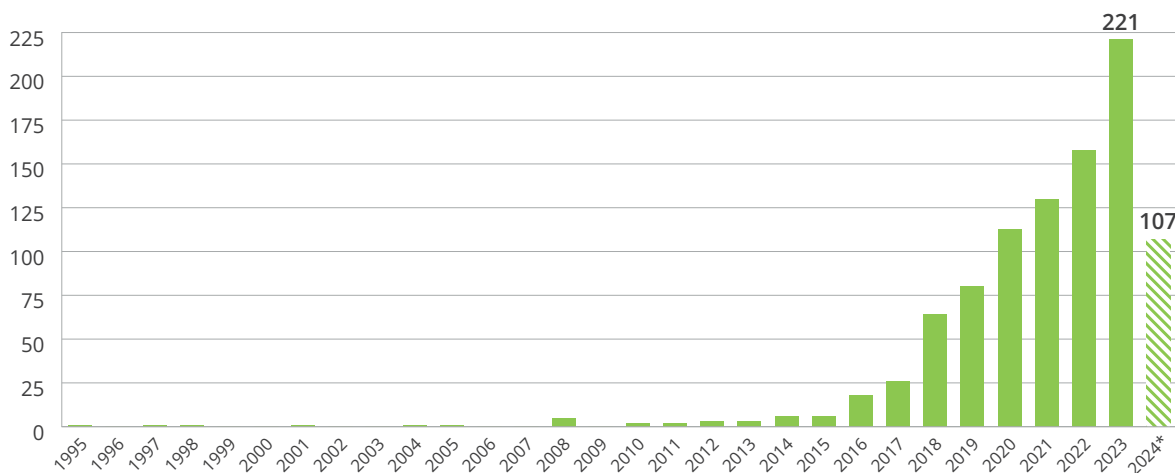
The drive to capitalize on promising clinical applications

The presence of AI in health care is growing rapidly. FDA authorizations of medical devices incorporating AI technology have increased significantly in recent years. 221 devices were authorized in 2023, and 2024 is on pace to match or exceed that number.¹

AI has the potential to revolutionize many aspects of patient care and clinical operations. One of the foremost benefits is the improvement in diagnostic accuracy. For example, AI algorithms could potentially detect smaller artifacts and irregularities in medical imaging scans that are often missed by the human eye. Researchers are exploring this use case and potential diagnostic capabilities using a variety of biometric data.²

Beyond diagnostics, AI also excels in managing and monitoring large, dynamic datasets that would be too expansive or time-consuming for humans to assess effectively. AI can use this capability to analyze both individual and population health data.

FDA submissions of medical devices incorporating AI and machine learning



*As of August 7, 2024
U.S. Food and Drug Administration

Practical forms of AI technology

Machine learning



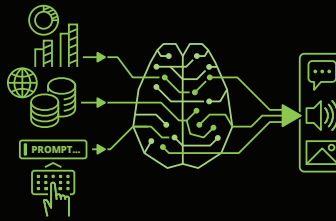
A field within AI that uses algorithms to enable computers to learn new information without manual programming.

U.S. Food and Drug Administration

Deep learning

The use of advanced neural networks to identify and analyze complicated patterns.

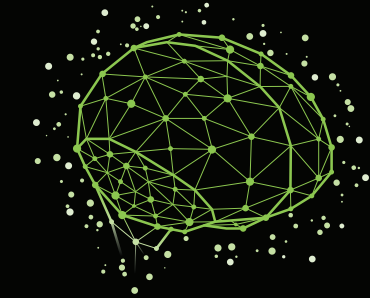
I. H. Sarker, Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions



Large Language Models (LLMs)

Machine learning modules that rely on their datasets to generate human-seeming content, whether that be text, audio, or visual elements.

Q. Ding et al., Unraveling the Landscape of Large Language Models: A Systematic Review and Future Perspectives



By identifying trends and warning signs for infectious and chronic diseases, AI enables healthcare providers to implement preventive measures and tailor treatments to individual patient needs.² This proactive approach improves patient outcomes and reduces the overall burden on healthcare systems.

Deploying AI to manage complex data could also include sizeable medical equipment inventories. AI may be able to ensure that critical medical devices are always operational by optimizing performance, expediting maintenance, balancing utilization, and predicting possible failures. This reliability is essential for advancing consistent and high-quality patient care.

AI can also improve patients' access to care resources and personnel by simplifying administrative work for clinicians and technicians. By automating routine tasks such as scheduling and documentation for various disciplines, AI software could free up valuable time for healthcare professionals. This allows them to focus more on direct patient care activities that contribute the most to improving the effectiveness and quality of care.

The arrival of AI in a complicated era for data security

Like any breakthrough technology, incorporating AI into clinical settings—where the stakes could not be higher—will alter the risks that patients and clinicians face. Not least among these is cybersecurity risk, which is already one of the most pressing challenges in modern health care.

The financial, operational, and safety damages that many health systems have experienced from cyberattacks have made security a top priority for health system leaders. Yet, the complexity and rapid evolution of healthcare technology mean that there are no simple solutions to this challenge.

AI is far from the only technological revolution that has impacted healthcare in the digital age. Network-connected medical devices and IT solutions have rapidly expanded in recent years. Digital technology's capabilities have helped overcome the hurdles that factors like location and human error pose to patient outcomes. Yet, a more connected inventory increases the potential attack surface in clinical environments. As AI technology proliferates in health care, it becomes an increasingly important aspect of this concern.

Cybersecurity is a crucial reason to establish a baseline understanding of what defines AI. Misconceptions about the capabilities and limitations can create gaps in how effectively risk factors are identified and assessed. John McCarthy, an early pioneer of AI, offered the following definition³:

[Artificial Intelligence] is the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable.

- John McCarthy, What is Artificial Intelligence?

McCarthy also indicates the challenges of establishing a universally applicable definition for this technology, as the term 'intelligence' itself is difficult to define.² Practical applications of AI encompass a range of technologies, each with unique applications and functions.

It is also crucial to distinguish between AI and software that only processes input data through algorithms to automate or streamline processes. While both can enhance efficiency, AI's ability to learn and adapt sets it apart, offering transformative potential in personalized medicine, predictive analytics, and more. However, this same adaptability adds an element of complexity to managing the risks of a new, evolving technology.

How expanding AI applications will complicate risk management

The healthcare industry is one of the leading targets for cyberattacks because of the sensitivity of electronic protected health information (ePHI) and the potential damage if it falls into the wrong hands. Protecting ePHI has been the priority of many legislative and regulatory initiatives, but evolving technology has made it difficult for industry standards and guidelines to keep pace.

The modern standard of care depends on appropriately storing, accessing, and sharing ePHI, which empowers clinicians to make faster, better-informed patient care decisions. Likewise, many AI applications in health care require access to ePHI to contribute to outcomes and efficiency. Yet every time a networked technology asset—including AI—is given access to ePHI, it creates a potential risk.

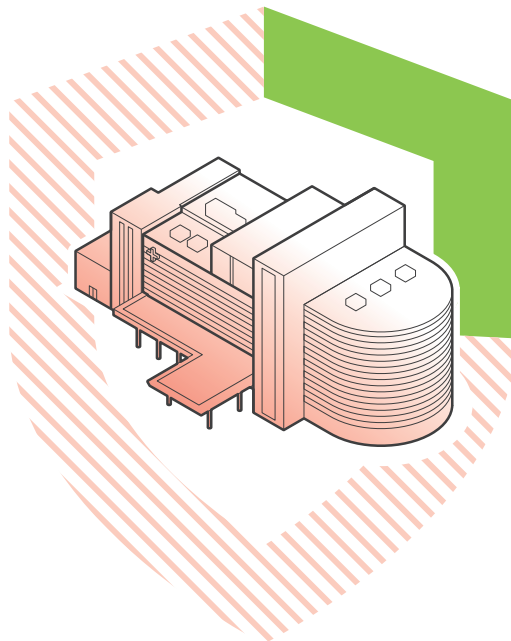
Some degree of risk is an inevitable part of applying evolving technologies in any industry. New software inevitably comes with vulnerabilities that attackers can exploit, and both users & manufacturers must take steps to address them. With the amount of technology used in healthcare settings, identifying, monitoring, and remediating vulnerabilities has become a bandwidth challenge for many organizations. The healthcare industry has felt what is now a global shortage of cybersecurity professionals needed to manage the persistent rise in cyberattacks. Research has indicated that 74% of healthcare organizations feel underequipped to meet their cybersecurity needs with their current staffing numbers.⁷

Health systems are showing uncertainty about their cybersecurity preparedness for a good reason. Over half of the network-connectable medical devices in hospital inventories have known critical vulnerabilities.⁸

This challenge is likely to grow even more pronounced as advanced software applications with AI capabilities become more prevalent in clinical settings and perform more substantial roles in care pathways. By adding another layer of networked digital technology to healthcare operations, the number of vulnerabilities and how attackers could exploit them could scale far beyond what many health systems' resources are equipped to handle.

The legitimate uses of AI are not the only factors that will impact healthcare cybersecurity concerns. Attackers will also seek to breach networks more effectively with these emerging technologies, including increasing the sophistication and efficiency of their methods.

74%
of health systems



feel underequipped to meet cybersecurity needs

Different aspects of AI technology present unique opportunities to hackers. For example, generative AI can remove the trade-offs of different types of phishing tactics. All phishing attacks rely on tricking targets into accessing malware or surrendering sensitive information with deceptive content and statements to grant access to an organization's network. However, attackers use unique approaches depending on their preference for precision or scale. For example, spear phishing foregoes sending one message to a large number of recipients, instead tailoring communications towards specific targets, whether that is one individual or a team within an organization. With generative AI tools, creating persuasive emails, text messages, or even voice impersonations becomes easier, less time-consuming, and more accessible to hackers.



The more involved an AI-driven technology is in patient care activities, the greater the risk.

Bad actors could also exploit legitimate AI applications' reliance on their foundational datasets and input accuracy. Just as ransomware attacks lock up technology and IT resources, an attacker who breaches a network could potentially disrupt data-driven AI by exploiting that dependency. In cases where a breach is identified and the affected organization is notified, this could substantially slow down clinical operations. However, if such a breach went undetected, this could result in threats to patient safety. The more involved an AI-driven technology is in patient care activities, the greater the risk.

To effectively manage these complex risk factors, health systems must find ways to fold AI vulnerabilities and characteristics into a cybersecurity strategy that prioritizes consistency, visibility, and continuous improvement. This best practice applies to all connected and connectable clinical technology—not just AI. There are overarching questions that organizations can use to grade the reliability of their current strategy:

1 How do we identify, document, and manage vulnerabilities to assess risk?

As discussed earlier, even cataloging vulnerabilities can challenge organizations with staffing shortages and extensive technology assets. This requires accurate equipment inventory records and sourcing new vulnerability data as it is released from industry and government groups. For AI applications and devices, this also means documentation of functionality to help identify potential anomalous behavior. Health systems can alleviate resource constraints by examining what tools can help their teams manage such a wealth of inventory and vulnerability data.

2 How do we create a risk register that properly quantifies and prioritizes risks associated with vulnerabilities?

Every organization has unique risk management needs. Understanding the greatest clinical needs and how they connect to high cybersecurity risk areas will help clarify the options for remediating vulnerabilities while maintaining clinical operations. It is essential to know and prepare for manufacturer-validated patches not to be immediately available, as can be the case with advanced technology solutions as well as older assets.

3 How do we equip our workforce to defend against evolving threats?

Since every networked technology touchpoint is a potential vector for a data breach, health systems require an organizational culture that prioritizes vigilance for all associates. This includes emphasizing the shared responsibility for cybersecurity and providing the tools to identify risk in everyday work. Regular training and education can strengthen personal security practices and keep associates aware of trends and emerging threats they can expect to face.

4 How do we show measurable improvements in our risk posture from cybersecurity initiatives?

Clear goals and success metrics are imperative for a cybersecurity program. This begins with quantifying risk and closes the loop by thoroughly documenting all vulnerability remediation activities. With full visibility of urgent organizational needs and outcomes, cybersecurity becomes a continuous, proactive process instead of disjointed, reactive projects.

How health systems can leverage AI to fight back against cyber risk

Asking questions that reveal the preparedness of a cybersecurity strategy for AI implementation can be daunting. However, technology solutions, including AI, can support these efforts. Health systems can significantly enhance cybersecurity measures by leveraging AI to monitor large inventories and device behavior, analyze vulnerability databases, and consistently assess cybersecurity risk.

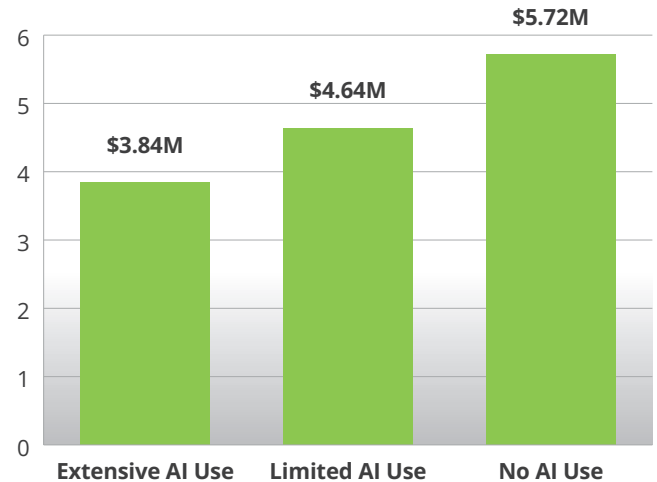
By integrating AI with computerized maintenance management systems (CMMS) and real-time monitoring programs, health systems can efficiently and continuously analyze the performance and behavior of their medical equipment inventory with less manual work. AI algorithms can process vast amounts of data from various medical devices, identifying patterns and anomalies that may indicate potential security threats. This continuous monitoring ensures that any unusual behavior is detected promptly, allowing immediate action to mitigate risks. For instance, AI can flag devices that deviate from their normal operating parameters, signaling a possible security breach.

AI cybersecurity integration can improve incident response and mitigate damages

Time needed to identify and contain data breaches



Cost of data breaches



IBM, Cost of a Data Breach 2024

AI can also streamline the process of analyzing vulnerability databases and matching them to the health system's inventory. By automating this process, health systems can quickly identify which devices are impacted by newly discovered vulnerabilities. This capability is crucial for maintaining up-to-date security measures, as it allows health systems to prioritize and address the most critical vulnerabilities first. AI can cross-reference vulnerability databases with the inventory data, ensuring no device is overlooked.

While consistent risk assessment is vital for maximizing the impact of a cybersecurity strategy, it can seem to be an overwhelming effort. AI can enhance this process by quickly reporting dynamic risk scoring based on real-time data. AI-driven risk assessment tools can help evaluate the potential impact of vulnerabilities, considering factors such as device criticality, network exposure, and historical threat patterns. This comprehensive risk assessment enables health systems to allocate resources effectively, focusing on the areas with the highest risk. Additionally, AI can simulate potential attack scenarios, helping health systems to understand their vulnerabilities better and prepare appropriate defense strategies.

The healthcare industry needs to adopt a proactive approach to investigating and uncovering risk, as is required with networked technology.

However, an important part of cybersecurity is preparing to handle any circumstance, not just successful prevention. If a breach occurs, teams equipped with AI tools and strong processes may be able to respond more effectively to help prevent harm to patients and technology assets. In an IBM report, surveyed organizations that incorporated AI tools in their cybersecurity program were able to reduce the time to identify and contain a breach by an average of 21–31%, depending on the level of AI usage. These comparisons also showed that using AI tools correlated with lower data breach costs, with an average difference of \$800,000 to \$1.77 million.⁹

The excitement around technological innovations like AI can sometimes overshadow the risks that health systems must manage carefully. At the same time, concerns over those risks can make the potential benefits of AI for patients, clinicians, and entire organizations seem unattainable. The actual impact depends on how AI is used and how carefully it is governed in clinical settings. The healthcare industry needs to adopt a proactive approach to investigating and uncovering risk, as is required with networked technology. Fortunately, process-driven cybersecurity policies and even tools with AI capabilities can be powerful tools for creating a successful path forward for health care in this technological frontier.

SOURCES

1. U.S. Food and Drug Administration. (2021). *Artificial Intelligence and Machine Learning (AI/ML)-Enabled Medical Devices*. FDA. <https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-aiml-enabled-medical-devices>
2. Davenport, T., & Kalakota, R. (2019). *The Potential for Artificial Intelligence in Healthcare*. *Future Healthcare Journal*, 6(2), 94–98. <https://doi.org/10.7861/futurehosp.6-2-94>
3. U.S. Food and Drug Administration. (2021). *Artificial Intelligence/ Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan*. FDA. www.fda.gov/media/145022/download
4. Brown, S. (2021). *Machine learning, explained*. MIT Sloan; MIT Sloan School of Management. <https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained>
5. Sarker, I. H. (2021). *Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions*. *SN Computer Science*, 2(6). Springer. <https://doi.org/10.1007/s42979-021-00815-1>
6. Ding, Q., Ding, D., Wang, Y., Guan, C., & Ding, B. (2023). *Unraveling the Landscape of Large Language Models: A Systematic Review and Future Perspectives*. *Journal of Electronic Business & Digital Economics*, 3(1), 3–19. <https://doi.org/10.1108/jebde-08-2023-0015>
7. ISC2. (2023). *How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce 2023*. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf
8. TRIMEDX internal data
9. IBM. (2024). *Cost of a Data Breach 2024*. IBM. <https://www.ibm.com/reports/data-breach>



Identify and secure your medical device cybersecurity risks

With more network-connected technology, higher costs from data breaches, and increasing frequency of attacks, health systems need to prioritize staying ahead of cyberattacks before they happen. Vigilor from TRIMEDX combines industry-leading technology, knowledge, and data with cybersecurity expertise to protect your medical devices from cybersecurity threats and reduce patient safety risks.



Proactively secure your clinical assets and patients.

vigilor.com



info@vigilor.com