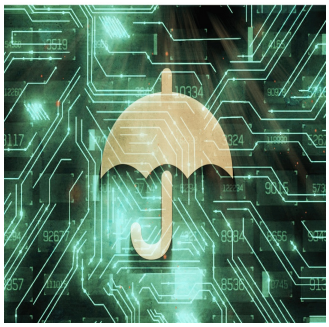
HealthManagement
Promoting Management and Leadership

Safeguarding Patient Care: Addressing Health Tech Risks in 2025



Healthcare technologies, ranging from sophisticated artificial intelligence (AI) systems to home-based medical devices, are pivotal in transforming patient outcomes. These tools enhance diagnostic accuracy, improve treatment protocols and optimise healthcare delivery processes. However, implementing and managing such technologies can introduce significant risks if not adequately addressed. The ECRI's 2025 report on health technology hazards offers an invaluable guide to identifying and mitigating these risks to safeguard patient safety. There are three main areas of concern—risks associated with AI-enabled technologies, unmet support needs for home care patients, and vulnerabilities linked to third-party vendors and cybersecurity threats. Proactive measures in these areas can help healthcare providers mitigate risks and protect patients.

Risks of AI-Enabled Health Technologies

AI has the potential to profoundly transform healthcare by augmenting clinical decision-making, enhancing operational efficiencies and expanding access to personalised care. Its applications in areas such as predictive diagnostics and treatment planning hold immense promise. However, the integration of AI into clinical practice comes with inherent risks. These arise primarily from the complexities of AI training and its interaction with real-world patient data.

A significant issue stems from biases in the data sets used to train AI systems. When these data sets fail to represent diverse patient populations, the resulting AI models may produce inequitable or inaccurate recommendations. Additionally, "data drift" and the brittleness of AI algorithms can lead to performance degradation over time, particularly when these systems encounter unfamiliar conditions. Misleading outputs, often referred to as "hallucinations," further underscore the importance of human oversight in AI-enabled care.

Moreover, overreliance on AI systems can exacerbate risks. Organisations frequently fail to establish robust governance frameworks or clear implementation strategies, often resulting in unrealistic expectations. Without regular monitoring, risk assessments and rigorous validation of AI outputs, the potential for harm increases significantly. For AI to fulfil its promise, it must act as a complementary tool that enhances—not replaces—critical human decision-making processes.

Supporting Home Care Technology Needs

The expansion of home-based healthcare services reflects a broader effort to decentralise care and improve accessibility. Home care technologies such as ventilators, dialysis machines and infusion pumps empower patients to manage their conditions in familiar environments. However, these devices also introduce unique challenges when used outside clinical settings, where professional supervision is absent.

One primary concern is the usability of these technologies by lay users, such as patients and family caregivers. Without sufficient training or technical support, these users may struggle with device setup, maintenance or troubleshooting. Mistakes in operation can lead to inaccurate readings, delays in care or device malfunctions—any of which can result in severe patient harm.

Further complications arise when device selection does not align with the specific needs of the patient or the constraints of their home environment. For instance, inadequate physical space, limited mobility or a lack of reliable power sources can impede the safe operation of equipment. Addressing these challenges requires a holistic approach encompassing usability testing, comprehensive user training and ongoing technical support.

Healthcare providers must also anticipate and mitigate risks proactively. This involves assessing the patient's capacity to operate medical devices, providing alternative solutions where necessary, and ensuring that caregivers have access to resources to manage emergencies. By prioritising support systems and education, the healthcare sector can enhance patient safety and enable more effective care in home settings.

Cybersecurity Threats from Vulnerable Vendors

As healthcare organisations increasingly rely on third-party vendors for critical services such as electronic health records, diagnostic systems and telemedicine platforms, the risk of cybersecurity breaches has grown exponentially. Disruptions caused by ransomware attacks or unauthorised access to third-party systems can compromise patient data, disrupt care delivery and erode public trust in healthcare institutions.

One notable concern is the interdependence of healthcare operations on these external vendors. A single cybersecurity incident at a vendor's facility can cascade into widespread service outages, leaving healthcare providers unable to access vital systems or communicate effectively with their partners. Such events not only delay care but can also lead to potentially life-threatening situations for patients.

To mitigate these risks, healthcare organisations must adopt a multi-faceted approach to cybersecurity. This includes conducting thorough risk assessments when selecting vendors, implementing robust data encryption and redundancy protocols and regularly testing incident response plans. Additionally, fostering collaboration between regulatory bodies, vendors and healthcare providers can help establish industry-wide standards for cybersecurity resilience.

By addressing vulnerabilities in vendor relationships and investing in preventative measures, healthcare organisations can safeguard their operations against external threats. Proactive management of cybersecurity risks ensures continuity of care and reinforces trust in the integrity of healthcare systems.

Integrating advanced technologies into healthcare offers unparalleled opportunities to improve patient outcomes and reorganise care delivery. However, these benefits come with corresponding risks that require careful attention and mitigation. Addressing the limitations of AI systems, supporting the effective use of home care technologies and strengthening cybersecurity frameworks are crucial steps in minimising potential harms. Collaboration among healthcare providers, policymakers and technology developers is essential to build resilient systems prioritising safety and equity. By focusing on these key areas, the healthcare sector can harness technological innovations while safeguarding the well-being of patients.

Source: ECRI
Image Credit: iStock

Published on : Mon, 9 Dec 2024