

CYBERSECURITY IN HEALTHCARE:

WHY PROTECTING PATIENT DATA HAS NEVER BEEN MORE CRITICAL

By Richard Preston, Preston Office Solutions

Healthcare organizations are at the forefront of a digital revolution, but with innovation comes risk. The rapid adoption of electronic health records (EHRs), telemedicine, and cloud-based platforms has created an environment where sensitive patient data is constantly in motion. Unfortunately, this also means cybercriminals have more entry points than ever before. According to the Department of Health and Human Services, healthcare data breaches affected over 100 million individuals in 2023, underscoring the urgency for robust cybersecurity measures.

One of the most significant challenges facing healthcare providers is resource allocation. Smaller hospitals and private practices often lack the budget and personnel to implement enterprise-grade security solutions, leaving them vulnerable to ransomware attacks, phishing schemes, and insider threats. Ransomware has become the most common type of cyberattack in healthcare, with criminals demanding exorbitant payments to restore access to critical systems. For providers, downtime can delay patient care and put lives at risk.

Recognizing these realities and understanding that many smaller medical offices struggle to afford robust protection, Preston Office Solutions has developed cybersecurity solutions that make enterprise-level safeguards accessible to any size practice. Rather than relying on reactive measures, they emphasize layered security strategies that include advanced firewalls, endpoint protection, and continuous monitoring. "Cybersecurity isn't a one-time project; it's an ongoing commitment," says Richard Preston. "Our goal is to give healthcare professionals peace of mind so they can focus on outcomes."

Education is another critical component of cybersecurity. Technology alone cannot prevent breaches if employees aren't trained to recognize threats. Preston Office Solutions provides tailored training programs that teach staff how to identify phishing

emails, secure mobile devices, and follow best practices for password management. This human-centric approach reduces the likelihood of accidental breaches, which remain one of the leading causes of data loss in healthcare.

Looking ahead, the integration of artificial intelligence and machine learning into cybersecurity frameworks offers promising opportunities. These technologies can detect anomalies in network traffic, predict potential vulnerabilities, and automate responses to threats in real time. However, implementing such solutions requires expertise and strategic planning—areas where managed service providers like Preston Office Solutions excel.

Ultimately, safeguarding patient data is not just a regulatory requirement; it's a moral obligation. Patients trust healthcare providers with their most intimate information, and that trust must be protected at all costs. By partnering with experienced technology providers, healthcare organizations can build resilient systems that withstand evolving cyber threats.

The bottom line: Cybersecurity is no longer optional; it's mission-critical. Healthcare leaders must act now to fortify their defenses.



Prosperity & Purpose

ABOUT THE AUTHOR

Richard Preston, owner and CEO of Preston Office Solutions in St. George, Utah, has been a trusted name in business technology for over forty years. Under his leadership, Preston Office Solutions has earned a solid reputation for exceptional sales, service, and support of office multifunction printers and large-format printing products across Southern Utah and southern Nevada. Preston Office Solutions is more than just a print solutions provider. As a dependable IT partner, the company delivers a comprehensive suite of technology products and services—all designed to support the success and growth of every client. To learn more, contact Preston Office Solutions at 435-628-2997 or visit www.prestonoffice.com.