



CYBERSECURITY SOLUTIONS FOR HEALTHCARE

Legacy Systems, IoT, and Compliance: Overcoming Healthcare's Security Hurdles with CyFlare

INTRODUCTION:

Healthcare providers are prime targets for cyberattacks. They handle vast stores of sensitive patient data (PHI) and require uninterrupted access to systems to ensure quality patient care. Yet, limited resources often restrict them from implementing the same cutting-edge defenses common in other industries.

DID YOU KNOW?

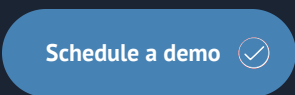
- The average healthcare data breach exposes over 57,000 records.1
• The healthcare industry has the highest average data breach cost at over \$10M per incident.2
• In 2022, the largest HIPAA settlement to date was \$16 million.3

CyFlare recognizes the unique security hurdles faced by healthcare organizations. We work tirelessly to simplify the complexities of securing connected medical devices, sprawling networks, legacy systems, and often fragmented inventories. Our mission is to empower healthcare providers to deliver exceptional patient care while safeguarding sensitive data, all within the framework of evolving HIPAA compliance standards.

Table with 2 columns: Healthcare Security Challenge and CyFlare Solution. Rows include Legacy Systems and IoT Proliferation, Resource Constraints, and Evolving Regulatory Landscape.

1 IBM Security Report 2023
2 IBM Security 2023 Cost of a Data Breach Report
3 Forbes, Healthcare Data: The Perfect Storm

Interested in Learning More?



Or get in touch: sales@cyflare.com

“Our 3,000-person healthcare organization needed to achieve SOC 2 Type II compliance within the year and continue to monitor our security and privacy against HIPAA. CyFlare got us up and running in 30 days, giving us clear visibility across our infrastructure, a 90%+ true positive rate to reduce alert fatigue, and high coverage against MITRE.”

- CIO, Large Midwestern Healthcare system

