Cybersecurity for Healthcare

While your healthcare organization is focused on providing critical care, improving the patient experience and exploring groundbreaking treatments and technologies, cyber criminals and threat actors are aggressively seeking out your vulnerabilities and looking for ways to attack. Dealing with highly sensitive data and private personal information, the healthcare industry is one of the most targeted, making up 15% of attacks, and leading cybersecurity and HIPAA compliance to be an ongoing concern. **Here are some alarming stats:**

By the end of 2020, security breaches are expected to cost healthcare companies ***$6 trillion dollars***. (PhoenixNAP)

Penalties for non-HIPAA compliance range from ***$100 to $50,000 per record***. (HIPAA Journal)

Lost or stolen protected health information (PHI) is estimated to cost the US healthcare industry up to ***$7 billion*** annually. (JAMIA)

Healthcare has the highest cost per breached data record of any industry, at ***$408/record*** - 3x the cross-industry average. (HIPAA Journal)

1,531,855 healthcare records were breached during 39 incidents in February 2020 alone. (HIPAA Journal)

Solutions to Address Common Challenges and Concerns

Unified Communication (UC) tools with built-in security and data protection along with HIPAA-compliant features allow for properly regulated telehealth programs, using voice, video, recording, and even EMR/EHR system integrations

Enterprise Mobility Management (EMM) solutions give security and visibility into mobile devices, protecting electronic health records (EHR) and sensitive information

Bring Your Own Device (BYOD) policies provide direct guidance on personal device usage; could include "must install" organization's endpoint security for all employees

Medical Endpoint Security offer proper ransomware, medical device protection and patch management

Infrastructure Audits ensure adherence to HIPAA Security Rule Section 164.308(a)(1)(ii) and that networks and physical servers stay protected against unauthorized parties accessing electronic protected health information (PHI)

Ongoing **HIPAA/HITRUST Training and Cybersecurity Education** help reduce security breaches caused by human error and remain in compliance

Network Access Control (NAC) provide network visibility and access management, enforcing policies across devices and users of corporate/healthcare networks. Capabilities include:

- Policy lifecycle management – Enforce policies for all operating scenarios without requiring separate products or additional modules
- Profiling and visibility – Recognize and profile users and their devices before malicious code can wreak havoc
- Guest networking access – Manage guests through a customizable, self-service portal that includes guest registration, guest authentication, guest sponsoring, and a guest management portal
- Security posture check – Evaluate security-policy compliance by user type, device type, and operating system
- Incidence response – Mitigate network threats by enforcing security policies that block, isolate, and repair noncompliant machines without administrator attention
- Bidirectional integration – Integrate with other security and network solutions through the open/RESTful API

Managed Security Services offer around the clock security handled by experts, remaining in compliance with all regulations and industry requirements

Find the right security solutions for healthcare.
Get a professional security assessment to help determine your organization's needs, identify vulnerabilities and provide recommendations on the best plan for action.

Email info@techguidance.com or call 855.898.0655.

techguidance
Powered by TBI