vertikal 6
TECHNOLOGY. ELEVATED.

Checklist

15 Ways to Protect Your Healthcare Practice From a Cyberattack

Phishing scams. Data breaches. Ransomware. In recent years, small medical offices became even bigger targets for cybercriminals, overwhelming the IT resources of smaller practices. That's why we've outlined some ways you can keep your cyber defenses sharp – as well as areas where an IT partner like Vertikal6 can provide targeted support where you need it most.

◯ Security Assessment

Establish the current security baseline for your office to close vulnerabilities. When was your last assessment? Click here and schedule a free consultation.

Date: _____

◯ Spam Email

38% of healthcare attacks originate from email; is your platform secure? We'll help you choose a service designed to reduce spam and your exposure to attacks on your staff via email. (Source: Health Sector Cybersecurity Coordination Center)

◯ Policies

Apply security policies on your network. Examples: Deny or limit USB file storage access, enable enhanced password policies, set user screen timeouts, and restrict user access.

◯ Security Awareness

It's easy for busy staff and clinicians to miss security basics. Teach them about data security, email attacks, and your policies and procedures. We offer a web-based training solution and "done for you" security policies.

◯ HIPAA & Other Compliance Risks

Are you up to date on the latest HHS standards for HIPAA? What about other relevant regulations, such as Sarbanes-Oxley and PCI DSS, that affect your office's workflow and procedures?

◯ Advanced Endpoint Detection & Response

Off-the-shelf antivirus programs don't cut it for medical offices today. Protect your computer's data from malware, viruses, and cyberattacks with advanced endpoint security. Update with advanced tech – it can even help protect against a ransomware attack.

◯ Electronic Health Records (EHR) Security

EHRs contain sensitive patient information and are a prime target for cybercriminals. We can help ensure your EHR system has strong access controls, encryption, and regular security audits.

◯ Multi-Factor Authentication

This usually involves receiving a code on a phone after entering your password – adding an important extra layer of security. Most systems have a simple option to turn this on.

◯ Telehealth Security

Make sure the telehealth platform you use is compliant with healthcare privacy laws and employs strong encryption protocols for both audio and video to protect patient confidentiality and data integrity.

Computer Updates

Keep Microsoft, Adobe, and Java products updated for better security. We provide a “critical update” service via automation to protect your computers from the latest known attacks.

Dark Web Research

Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach. We scan the Dark Web and take action to protect your business from stolen credentials that have been posted for sale.

Web Gateway Security

Internet security is a race against time. Cloud-based security detects web and email threats as they emerge on the internet and blocks them on your network within seconds – before they reach the user.

Mobile Device Security

In a modern work-from-anywhere healthcare setting, today’s cybercriminals attempt to steal data or access your network by way of your staff phones and tablets. They’re counting on you to neglect this piece of the puzzle. Mobile device security closes this gap.

Encryption

Whenever possible, the goal is to encrypt files at rest, in motion (think email), and especially on mobile devices.

Backup

Backup local. Backup to the cloud. Have an offline backup for each month of the year. Test your backups often. And if you aren’t convinced your backups are working properly, call us ASAP.

Don’t take chances with your patients’ data.

Schedule a Free Cybersecurity Assessment for Your Office Today.

Did You Know?

10%

increase in cyberattacks on physician groups since 2021.

Source: Critical Insight/Department of Health & Human Services.

104%

increase in healthcare cyberattacks in 2023.

$11 million

average cost of a healthcare data breach in 2023.

Source: Becker’s Hospital Review, Aug. 22, 2023.

$77 billion

cost of healthcare ransomware attacks on the US economy in 2023.

Source: Becker’s Health IT, Oct. 26, 2023.

Vertikal6 is on a mission to bring enterprise-level IT services and expertise to small organizations, including healthcare practices. Whether you need cybersecurity, IT outsourcing, help desk, IT professional services, hosting, or software development, we’re here to help healthcare clients maximize revenue and uptime. Learn more at www.vertikal6.com.

PHONE: 401-825-4401 **EMAIL: INFO@VERTIKAL6.COM**

vertikal 6 TECHNOLOGY. ELEVATED.