PRONTOTECH

Cybersecurity Checklist for **Healthcare Providers**

Stay protected by following these steps:

□ Complete Healthcare Cybersecurity Assessments

Conduct regular audits of your network, devices, systems, and data to identify vulnerabilities and gaps. Use tools such as the Health Industry Cybersecurity Practices (HICP) guide or the COVID-19 Checklist from CISA to evaluate your current security posture and compliance status.

□ Develop an Incident Response Plan

Prepare for potential cyber incidents by creating a clear plan that defines roles, responsibilities, procedures, communication channels, and recovery strategies. Test and update your plan periodically to ensure its effectiveness and alignment with best practices.

□ Create a Secure Network

Implement network security measures such as firewalls, encryption, VPNs, segmentation, monitoring, and logging to prevent unauthorized access or data breaches. Use secure protocols such as HTTPS and SSL/TLS for data transmission. Avoid using public Wi-Fi or unsecured devices for accessing sensitive information.

□ Ensure VoIP Phones Are Encrypted

Voice over Internet Protocol (VoIP) phones are often overlooked as a potential entry point for cyberattacks. Make sure your VoIP phones are encrypted using strong algorithms such as AES-256 or SRTP. Also configure your VoIP system to use secure authentication methods such as certificates or tokens.

□ Use Multi-factor Authentication (MFA)

MFA adds an extra layer of security by requiring users to provide more than one piece of evidence to verify their identity before accessing a system or data. MFA can use factors such as passwords, PINs, biometrics, tokens, or codes sent via email or SMS. Enable MFA for all accounts that access sensitive information or systems.

□ Train Your Staff

Human error is one of the most common causes of cyber incidents in healthcare settings. Educate your staff on how to recognize and avoid phishing emails, malware infections, ransomware attacks, and other common threats. Teach them how to use strong passwords, report suspicious activities, and follow security policies and procedures.

□ Enable Auto-Lock for Devices

Mobile devices such as laptops, tablets, smartphones, and USB drives can be easily lost or stolen, exposing sensitive data to unauthorized parties. Enable auto-lock features that require a password or biometric verification to unlock the device after a period of inactivity. Encrypt the data stored on these devices and enable remote wipe capabilities in case they are compromised.

□ Purchase Healthcare Cybersecurity Insurance

Cybersecurity insurance can help cover the costs associated with a cyber incident, such as legal fees, fines, ransom payments, data recovery, and reputation management. However, cybersecurity insurance does not replace the need for implementing robust security measures; it only provides financial assistance in case of an emergency. Choose an insurance policy that suits your specific needs and budget.