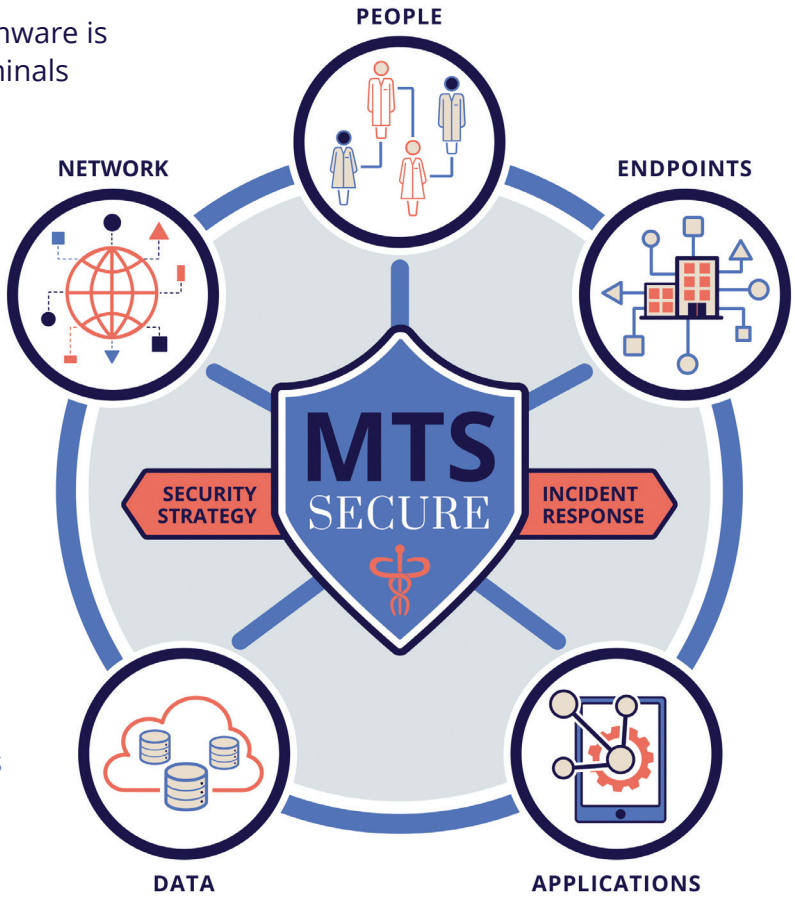
Med Tech Solutions

Ransomware Prevention & Preparation Checklist for Healthcare Organizations

Cyber challenges in the healthcare industry are impacting an already over-taxed environment. While every business is a potential target for a security breach, healthcare is especially at risk and continues to be the most-breached sector in 2021. (SOURCE: Herjavec Group)

To take the most appropriate actions and continue to provide care and generate revenue, IT leaders in healthcare organizations like yours need to understand your risks, reduce vulnerabilities, and apply controls to help protect your interests and data.

The need to protect your business from ransomware is ongoing and guidance can change as cybercriminals develop new capabilities and uncover new vulnerabilities. The following Ransomware Prevention and Preparation Checklist is based on current NIST and Med Tech Solutions best practice recommendations. We suggest that you implement these checklist items and work with a managed service provider with strong security expertise to ensure you have the necessary controls in place to protect against and prepare for potential ransomware events.



MTS Secure is a comprehensive security framework that underlies every service we provide.

RANSOMWARE PREVENTION & PREPARATION CHECKLIST

Know and document where your data is located

- ☐ Maintain up-to-date inventory of all hardware and authorized and unauthorized software
- ☐ Inventory where data is stored and its criticality (paper, digital, and proprietary storage):
  - ☐ *HIPAA/patient data*
  - ☐ *Employee records*
  - ☐ *Financial records*
  - ☐ *Corporate records*

Use endpoint detection and response (EDR) software at all times on all systems

- ☐ Scan all email
- ☐ Scan all drives

Keep all computers and systems fully patched

- ☐ Minimize the time between patch releases and fully patching devices
- ☐ Patch servers and network devices as well as workstations
- ☐ Actively scan for vulnerabilities

Apply DNS filtering

- ☐ Use security products or services to block access to known malware sites (email, web browsing, or other)

Allow only authorized applications

- ☐ Configure operating systems to allow only authorized applications
- ☐ Configure third-party software to allow only authorized applications
- ☐ Develop a process for software authorization and tracking
- ☐ Do not allow the use of personal applications on work systems (personal email, chat, social media)

Restrict personally owned devices on networks

- ☐ Enforce only authorized devices on the business network
- ☐ Enforce separation of devices based on need to access information

Ensure user-access controls

- ☐ Require multi-factor authentication (MFA) for remote access and web-based applications
- ☐ Restrict administrative privileges
- ☐ Require role-based access with least-privilege goal
- ☐ Document and audit the appropriate use of accounts

Beware of unknown sources

- ☐ Train employees to identify SPAM, phishing and other malicious email
- ☐ Patch servers and network devices as well as workstations
- ☐ Train employees to identify SMSishing, vishing, and instant messaging as part of social engineering training

RANSOMWARE PREVENTION CHECKLIST

Ensure backup and restoration

- ☐ Plan and implement a data backup and restoration strategy
- ☐ Ensure backups are isoloated from the production network
- ☐ Conduct disaster-recovery testing for backups

Create an incident management and recovery plan

- ☐ Define who is on the incident-response team
- ☐ Define roles for all those involved
- ☐ Define incident-response strategy and phases

Maintain active contact list

- ☐ Maintain accurate, up-to-date internal and external incident-response tean contact information
- ☐ Include local police, FBI, and other law enforcement
- ☐ Include this list as part of the incident-response plan

When you need help, turn to the experts

Med Tech Solutions creates technology systems that work the way healthcare practices work. Our Practice-Centered Care™ services are supported by dedicated IT Care Teams to ensure technology systems support essential clinical workflows and strategic business plans. Provider organizations and networks can count on a secure, reliable IT infrastructure, optimized clinical and business applications, and full end-user support so they can focus on patient care. MTS was founded in 2006 in Valencia, California, and serves thousands of healthcare practices nationwide. The company has been recognized as a seven-time Inc. 5000 Fastest Growing Private Company and the top Channel Futures MSP 501 provider for healthcare, and it has achieved HITRUST Common Security Framework (CSF) certification for its cloud platform.

Contact us for help on securing your network, applications, PHI, and other data at 877.687.1222 or info@medtechsolutions.com.