MEDCURITY RANSOMWARE CHECKLIST

Here are a few things you can proactively do to set your organization for success against ransomware attacks:

CYBER INSURANCE

It is becoming more and more prevalent for organizations to secure a Cyber Insurance policy to assist with something unexpected.

POLICIES & PROCEDURES

Protection against ransomware starts with a strong foundation developed of policies and procedures. HIPAA requires an annual Security Risk Assessment which typically includes a 3rd party review of those policies as it relates to the administrative, technical, and physical safeguards. Develop an action plan to address "opportunities" as a result of the Security Risk Assessment. These pieces of your HIPAA Compliance Program can help put safeties in place to protect your organization against attacks as well as OCR penalties.

HAVE A PLAN IN PLACE

Developing a Strong Contingency Plan or Business Continuity Plan is Key. Data Backup Plan – Develop a robust, reliable, and redundant data backup plan. Plan for onsite redundancy and offsite cloud. Test, Test and Test again. Develop a Disaster Recovery Plan. Emergency Preparedness plan. Role-based scenario testing.

PROTECT YOUR NETWORK

Implement Firewalls to tightly control access to other networks. Leverage Firewall technologies that have built-in antivirus / antispyware. Leverage Firewall technologies that have built-in content management. Implement Spam Filter software to detect/block unwanted emails.

PROTECT YOUR ENDPOINTS

Install managed antivirus / antispyware software. Keep up to date with Operating System Updates. Keep up to date with Software Updates. Ensure users do not have administrative rights to their workstations. Do not support end-of-life products (OS / Software / ETC)

TRAIN YOUR EMPLOYEES

It's critical to remember that the weakest link in any organizational cybersecurity defense is almost always the users. Your employees can't protect themselves if they haven't been trained how to.