CYBER SECURITY

Protecting your organization from cyber threats and data breaches is critical, especially for those who deal in sensitive information like HIPAA data. There are several things you need to be aware of and to be sure everyone else in your office is also aware.

1. Have a strong Email Security Gateway that has the following Five Key Features:
   a. Basic security (antivirus, antimalware, antiphishing and antispam)
   b. Advanced security (DPL, encryption)
   c. Management
   d. False positive rate that is acceptable
   e. Attachments processed and stored externally
2. Of the major gateway providers, i.e. Cisco, McAfee, Microsoft Exchange Symantec and others, the Providers that have these five key features are ;
   a. FortiMail
   b. Symantec Email Security Cloud
   c. Trend Micro InterScan Messaging Security.
3. Things you can do within Outlook to minimize threats.
   a. Set your Outlook options for Junk mail at High to move most of your junk mail to the Junk E-mail folder.
   b. Use Block Sender
   c. Set up a Blocked Sender list
   d. Create Rules for sorting, moving and more
   e. Use the rules wizard
   f. Check spam folders often
   g. Be sure you have the preview pane set up in Outlook. This will allow you to preview your messages before you open them.
   h. AND NEVER, EVER, EVER click on a link unless you know the sender and can be sure it is a valid link. It only takes one person to infect the whole network.
4. Firewalls should have the proper initial configuration, but maintenance is crucial. Best brands for less than 500 users are SonicWall, WatchGuard. You can also contract Firewall as a service for on-going maintenance and monitoring
5. Be sure that all your devices have the latest updates installed. Did you know this includes your scanners, copiers and printers?
6. Encrypt all sensitive files to protect from data breaches.
7. Enforce password policies and use strong passwords.

   Passwords should **NOT** include the following:
   • Personal information such as birthdates, addresses, phone numbers, or names of family members, pets, & friends
   • Work-related information such as building names, system commands, sites, companies, hardware, or software
   • Number or letter patterns such as *aaabbb*, *qwerty*, *zyxwvuts*, or *123321*
   • Common words spelled backward or preceded or followed by a number such as *terces*, *secret1*, or *1secret*

   Do not use the same password for business accounts and also for personal accounts
   • All system-level passwords should be changed at least quarterly
   • All user-level passwords should be changed at least every four months
   • Passwords must not be shared with anyone
   • Never reveal passwords over the phone
   • Do not use the “Remember Password” feature in apps or browsers
   • In case of suspected breach, change all passwords immediately