7 Urgent Security Protections Every Practice Should Have In Place Now

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium practices that are "low hanging fruit."
Don't be their next victim!
This report will get you started in protecting everything you've worked so hard to build.

Provided By: **Tier3MD** – IT Support for the HealthCare Industry
Author: SHERYL CHERICO, CEO
3690 N. Peachtree Rd. • Suite 100 • Atlanta, GA 30341
Tier3MD.com • 855-MyTier3 (698-4373)

Are You A Sitting Duck?

You, the Practice Administrator of a small medical group, are under attack. Right now, extremely dangerous and well-funded cybercrime rings in China, Russia and the Ukraine are using sophisticated software systems to hack into thousands of small practices like yours to steal credit cards, client information, and swindle money directly out of your bank account. Foreign governments are even funding some hackers to attack American businesses.

Don't think you're in danger because you're "small" and not a big target like a Emory or Piedmont Hospitals? Think again. 82,000 NEW malware threats are being released every single day and HALF of the cyber-attacks occurring are aimed at small practices; you just don't hear about it because it's kept quiet for fear of attracting bad PR, lawsuits, data-breach fines and out of sheer embarrassment.

In fact, the National Cyber Security Alliance reports that one in five small practices have been victims of cybercrime in the last year – and that number is growing rapidly as more practices under HIPAA must utilize cloud computing, mobile devices and store more patient information online. You can't turn on the TV or read a newspaper without learning about the latest online data breach, and government fines and regulatory agencies are growing in number and severity. **Because of all of this, it's critical that you have these 7 security measures in place.**

1. **Train Employees On Security Best Practices.** The #1 vulnerability for business networks are the employees using them. It's extremely common for an employee to infect an entire network by opening and clicking a phishing e-mail (that's an e-mail cleverly designed to look like a legitimate e-mail from a web site or vendor you trust). If they don't know how to spot infected e-mails or online scams, they could compromise your entire network.

2. **Create An Acceptable Use Policy (AUP) That Is HIPAA Compliant – And Enforce It!** An AUP outlines how employees are permitted to use practice-owned PCs, devices, software, Internet access and e-mail. We strongly recommend putting a policy in place that limits the web sites employees can access with work devices and Internet connectivity. Further, you have to enforce your policy with content-filtering software and firewalls. We can easily set up permissions and rules that will regulate what web sites your employees access and what they do online during practice hours and with practice-owned devices, giving certain users more "freedom" than others.

Having this type of policy is particularly important if your employees are using their own personal devices to access company e-mail and data.

If that employee is checking unregulated, personal e-mail on their own laptop that infects that laptop, it can be a gateway for hackers to enter YOUR network. If that employee leaves, are you allowed to erase company data from their phone? If their phone is lost or stolen, are you permitted to remotely wipe the device – which would delete all of that employee's photos, videos, texts, etc. – to ensure YOUR patients' information isn't compromised?

Further, we know that the data in your organization is highly sensitive, such as patient records, credit card information, financial information and the like, so you are not legally permitted to allow employees to access it on devices that are not secured; but that doesn't mean an employee might not innocently "take work home." If it's a company-owned device, you need to detail what an employee can or cannot do with that device, including "rooting" or "jail breaking" the device to circumvent security mechanisms you put in place.

3. **Require STRONG passwords and passcodes to lock mobile devices.** Passwords should be at least 8 characters and contain lowercase and uppercase letters, symbols and at least one number. On a cell phone, requiring a passcode to be entered will go a long way toward preventing a stolen device from being compromised. Again, your network administrator can ENFORCE this so employees don't get lazy and choose easy-to-guess passwords, putting your organization at risk.

4. **Keep Your Network Up-To-Date.** New vulnerabilities are frequently found in common software programs you are using, such as Microsoft Office; therefore it's critical you patch and update your systems frequently. If you're under a Managed IT Plan, this can all be automated for you so you don't have to worry about missing an important update.

5. **Have An Excellent Backup.** This can foil the most aggressive (and new) ransom-ware attacks, where a hacker locks up your files and holds them ransom until you pay a fee. If your files are backed up, you don't have to pay a crook to get them back. A good backup will also protect you against an employee accidentally (or intentionally!) deleting or overwriting files, natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters. Again, your backups should be AUTOMATED and monitored; the worst time to test your backup is when you desperately need it to work!

6. **Don't allow employees to download unauthorized software or files.** One of the fastest ways cybercriminals access networks is by duping unsuspecting users to willfully download malicious software by embedding it within downloadable files, games or other "innocent"-looking apps. This can largely be prevented with a good firewall and employee training and monitoring.

7. **Don't Scrimp On A Good Firewall.** A firewall acts as the frontline defense against hackers blocking everything you haven't specifically allowed to enter (or leave) your computer network. But all firewalls need monitoring and maintenance, just like all devices on your network. Your IT person or IT company, as part of their regular, routine maintenance too should do this.

Want Help In Implementing These 7 Essentials?

If you are concerned about employees and the dangers of cybercriminals gaining access to your network, then CALL US about how we can implement a managed security plan for your business.

At no cost or obligation, we'll send one of our security consultants and a senior, certified technician to your office to conduct a **FREE Security And Backup Audit** of your company's overall network health to review and validate different data-loss and security loopholes, including small-print weasel clauses used by all 3rd-party cloud vendors, giving them zero responsibility or liability for backing up and securing your data. We'll also look for common places where security and backup get overlooked, such as mobile devices, laptops, tablets and home PCs. At the end of this free audit, you'll know:

- Is your network really and truly secured against the most devious cybercriminals? And if not, what do you need to do (at a minimum) to protect yourself now?

- Is your data backup TRULY backing up ALL the important files and data you would never want to lose? We'll also reveal exactly how long it would take to restore your files (most people are shocked to learn it will take much longer than they anticipated).

- Are your employees freely using the Internet to access gambling sites and porn, to look for other jobs and waste time shopping, or to check personal e-mail and social media sites? You know some of this is going on right now, but do you know to what extent?

- Are you accidentally violating any PCI, HIPAA or other data-privacy laws? New laws are being put in place frequently and it's easy to violate one without even being aware; however, you'd still have to suffer the bad PR and fines.

- Is your firewall and antivirus configured properly and up-to-date?

- Are your employees storing confidential and important information on unprotected cloud apps like Dropbox that are OUTSIDE of your backup?

I know it's natural to want to think, "We've got it covered." **Yet I can practically guarantee my team will find one or more ways your practice is at serious risk for hacker attacks, data loss and extended downtime – I just see it all too often in the Medical Practices we've audited over the years.**

Even if you have a trusted IT person or company who put your current network in place, it never hurts to get a 3rd party to validate nothing was overlooked. I have no one to protect and no reason to conceal or gloss over anything we find. If you want the straight truth, I'll report it to you.

You Are Under No Obligation To Do Or Buy Anything

I also want to be very clear that there are no expectations on our part for you to do or buy anything when you take us up on our **Free Security And Backup Audit**. As a matter of fact, I will give you my personal guarantee that you won't have to deal with a pushy, arrogant salesperson because I don't appreciate heavy sales pressure any more than you do.

Whether or not we're a right fit for you remains to be seen. If we are, we'll welcome the opportunity. But if not, we're still more than happy to give this free service to you.

You've spent a lifetime working hard to get where you are. You earned every penny and every patient. Why risk losing it all? Get the facts and be certain your business, your reputation and your data are protected. Call us at 855-698-4373 or you can e-mail me personally at Sheryl.Cherico@tier3md.com.

Dedicated to serving you,

Sheryl Cherico, CEO
Web: www.Tier3MD.com
E-mail: sheryl.cherico@tier3md.com

Here's What A Few Of Our Clients Have Said:

Quick, Efficient and Knowledgeable

Medical Association of Georgia

Renai Lilly
Medical Association of Georgia
Atlanta, GA

"We depend on Tier3MD for our IT support needs. The customer service and care is always quick and efficient. The adept skills, knowledge, and swift communication from the Tier3MD support team make them a pleasure to work with. Thank you to the team for always being a short phone call away to alleviate any issues we experience."

Tier3MD Understands the Medical Space and Has Been Our Partner Through Substantial Growth

"I have had the pleasure of working with Tier3MD for the past eleven years. We hired them to support a large Oncology practice after outgrowing the internal IT department. Tier3MD cleaned up the network, infrastructure, and daily IT operations.

WOOLFSON EYE INSTITUTE

Marc Gilpin
Chief Financial Officer
Wolfson Eye Institute
Atlanta, GA

I transitioned to Woolfson Eye Institute in 2007 and found the incumbent network and IT service to be subpar. Therefore, I immediately called Tier3MD, and they quickly assessed our needs and built a network that could handle the growth of our practice (from 30 to 150 employees). Tier3MD has been our partner through substantial growth.

Tier3MD understands the medical space, easily assimilates into our environment, provides 24x7 service, and has great insight and strategies to offer. They are a great partner and have been a vital asset when executing projects such as an EMR rollout, phone system upgrade, equipment refresh, and new office build-out. I highly recommend Tier3MD."

Their Quick Response and Proactive Approach Made Our Technical Problems Go Away

BEAUFORT PEDIATRICS

Cheryl Gollihugh
Administrator
Beaufort Pediatrics
Beaufort, SC

"The lingering technical problems that we were experiencing finally went away when we switched to Tier3MD. They are incredibly proactive, and resolve problems before they become issues. Tier3MD has comprehensive knowledge of the medical community, especially with PM and EMR systems. Their solutions-oriented approach and quick response time are vital to our practice. I highly recommend Tier3MD to any medical practice."