ACUPUNCTURE Today

YOUR PRACTICE / BUSINESS

Cyber Threat Checklist: Defend Your Business With These 10 Steps

Daniel Ruscigno

Living in an internet connected society brings many conveniences and benefits. The power of the internet to connect us with customers, store data, and find information has opened the door for many small business owners to grow and flourish. But along with the benefits of this connectivity comes a responsibility to ensure the security of our businesses and our patient data.

One step you can take to keep your patient records secure is using a clinic management program that follows all of the guidelines laid out by HIPAA. This will take much of the burden of protecting personal health information (PHI) off of you. But what about the rest of the information storage systems used for your business? Any weakness in your security can leave you vulnerable to a cyber crime. Fortunately, there are steps you can take to prevent your acupuncture business from being victimized. I've listed several of these steps below.

10 Proactive Cyber Security Steps You Can Take Today

1. Password-protect your devices. Portable devices enable acupuncturists to take their data with them when visiting patients, but they also pose a substantial security risk. A 2016 article by SC Magazine reported that over one-quarter of data breaches that have occurred since 2006 were related to lost or stolen mobile devices. Don't let a lost or stolen device damage your business's reputation. Just like any data storage system (including your laptop/computer), your tablet or smartphone should be secured with a strong password.

2. Use unique passwords. No one really likes dealing with passwords and multi-step authentication. This is especially true when you are using multiple devices or workstations and need a different password for each one. Despite the hassles, using unique passwords and updating them regularly is still a necessary measure for keeping your business's data secure. If you resort to using a single password for all your devices, cyber criminals may exploit your password fatigue for their benefit.

3. Store your passwords securely. Keeping track of unique passwords can be a challenge. Many people report to writing them down in a Word or Excel document. Do not do this! If remembering passwords has become a challenge, look into using a password management program like LastPass.

4. Watch where you put things. One simple but often overlooked step to keep your data safe is to limit who has physical access to your data. Don't place networked devices in locations that are accessible to people visiting your office. If your family members share your device, create a separate login for them so your files are not accessible to them.

5. Keep your Wi-Fi activity private. If you use a Wi-Fi router in your office, secure your network by requiring a password to join. If you provide Wi-Fi access to your patients, you may want to chat with a technical expert to setup a guest network so that you are the only one with

access to the network you are using to work with PHI. If you access business or patient information from your home via Wi-Fi, employ these same protective measures there too.

6. Install antivirus software and use it. Malicious websites, shared files, and emails can all harbor malware that can harm your computers or steal your data. To protect against these hidden dangers, install antivirus software on you devices and update it regularly. Set your antivirus software to scan each email and download and to conduct regular scans of each computer to check for threats.

7. Store your files in the cloud. A lost or stolen device can be a nightmare as it could mean a loss of all of your patient files. By using a cloud-based practice management software program, your files will be stored securely on a central server. This means that if your device is lost or stolen your files are still safe. You can also look into services like Google Drive or Dropbox. Be sure to check the service providers HIPAA policy.

8. Backup your data. This is another item that's easily handled if you're using clinic management software, as the service provider will typically handle backups for you. If you are manually managing your files, you want to protect against damage or a lost/stolen device. You should make a copy of all of your patient files and storing them in another secure location.

9. Educate your staff. Your cyber security efforts will only be effective if every person in your office follows every security measure. It isn't just new hires that may need to be briefed. You should also schedule regular meetings with staff to review your policies and ask about any suspicious activity they may have noticed. In particular, remind your staff about the dangers of unauthorized software, password sharing, and leaving mobile devices unattended. Read through the HIPAA regulations and be sure you have no security holes in your day-to-day processes.

10. Ask an expert for advice. While some cyber security measures can be accomplished without assistance, you may find it useful to call in an expert. A professional in cyber security can perform an audit to identify weaknesses in your current practices. An expert can also help you secure your router and other equipment and advise you on best practices for ongoing safety.

A little prevention can go a long way when it comes to securing your organization's data. It can also save you a lot of money, as you may be subject to financial penalty if there is a data breach and you did not have acceptable security measures in place. By taking proactive steps to prevent a breach, you'll enhance your acupuncture practice's cyber security and gain peace of mind.

JULY 2018