

10-Point Cybersecurity Checklist for Medical and Dental Practices

Medical and dental practices rely on technology every day. Patient records, billing systems, email, scheduling, and communication all depend on computers and secure networks.

That also means cybersecurity is no longer just an IT issue. It is part of protecting your patients, your staff, and your practice.

Here are 10 important cybersecurity areas every medical and dental office should review.

1. Use Multi-Factor Authentication

Multi-factor authentication, or MFA, adds another layer of security beyond a password.

Even if someone steals a password, MFA can make it much harder for them to access your email, Microsoft 365 account, patient information, or other important systems.

Turn on MFA wherever possible, especially for email, cloud services, and administrative accounts.

2. Use Strong, Unique Passwords

Employees should avoid using the same password for multiple accounts.

If one password is stolen and reused elsewhere, a cybercriminal may be able to access more than one system.

Strong, unique passwords and a reputable password manager can make account security much easier to manage.

3. Keep Computers and Software Updated

Software updates often include important security fixes.

Older computers and unsupported software may no longer receive those updates, which can create security risks.

Make sure computers, servers, software, and other devices are regularly reviewed and updated.

4. Protect Every Computer and Device

Every device connected to your business network should have appropriate security protection.

Antivirus and Endpoint Detection and Response, or EDR, can help identify and respond to suspicious activity.

This includes office computers, laptops, servers, and other devices used for business.

5. Back Up Important Data

Backups are extremely important, but simply having a backup is not enough.

Your practice should also test backups to make sure important data can actually be restored.

Ask yourself this question: if your systems went down today, how quickly could you recover patient records and other important information?

6. Train Your Staff

Employees are an important part of cybersecurity.

Staff should know how to recognize phishing emails, suspicious links, fake payment requests, and unusual messages.

They should also know who to contact immediately if something does not look right.

Regular, simple training can help prevent costly mistakes.

7. Control Who Has Access

Not every employee needs access to every file or system.

Give employees only the access they need to perform their jobs.

When someone leaves the practice, disable their accounts and remove access as soon as possible.

Regularly reviewing user access can help reduce unnecessary security risks.

8. Secure Your Network and Wi-Fi

Your business network should be protected by a properly configured firewall.

Guest Wi-Fi should also be kept separate from the network your staff uses for patient records, billing systems, and other important business information.

This allows patients and visitors to use Wi-Fi without giving them access to your internal network.

9. Have an Incident Response Plan

If a cyberattack or security problem happens, your team should know what to do.

Your incident response plan should explain who to contact, how to respond to the problem, how to protect important systems, and how to begin recovery.

Having a plan before an emergency happens can help your practice respond more quickly and with less confusion.

10. Review Your Cybersecurity Regularly

Cybersecurity is not something you set up once and forget.

Your practice should regularly review computers, user accounts, backups, software updates, email security, network security, and access permissions.

As your practice grows and technology changes, your cybersecurity should change with it.

Final Thoughts

Medical and dental practices handle sensitive patient and business information every day.

Good cybersecurity does not have to be complicated, but it does require regular attention.

Start with the basics: protect your accounts, secure your devices, back up your data, train your staff, and have a plan for when something goes wrong.

The goal is simple: reduce risk, protect patient information, and keep your practice running.

Contact Best IT Guru today to review the cybersecurity of your medical or dental practice.

Follow Best IT Guru for more cybersecurity tips.

www.Bestitguru.com

610-600-1985