TECHNOLOGIES
COLOSSIANS 3:23

Top 10 Dental IT Best Practices

Whether you are working alone or have an IT company providing services for your practice or DSO. Here are the Top 10 Dental IT Best practices you can review in your organization.

1. FORMAL RISK ASSESSMENT

You must do a formal risk assessment and have a Health Insurance Portability and Accountability Act (HIPAA) risk management plan in place. You wouldn't treat a patient without doing a diagnostic workup and presenting a treatment plan, and HIPAA works the same way. You can't know where you're falling short of the rules, regulations, and best practices until you formally perform the risk assessment.

2. BACKUP DISASTER 7 RECOVERY

Set up a secure and compliant backup and disaster recovery system. If a patient goes to 5 different dentists, they're going to get 5 different treatment plans, and the same is true for dentists working with information technology (IT) providers. That being the case, your protocol at the very least should involve a local backup of the entire server (also known as an image), and both an onsite and offsite backup. Most organizations stop here, but backups can get corrupted. Regular testing and verification and restoring of test files should be done at a minimum, once a month.

3. UPDATES & PATCH MANAGEMENT

Keep all your software current and up to date. It's not just smart, it's the law and is called patch management. This is usually best done by an IT company. Although you can patch Windows on your own, I don't recommend that. Most offices have dozens of software programs they use, and manually patching all of those on your own is complex and time-consuming.

4. ENCRYPTION

Encrypt every device that contains electronic protected health information (ePHI). At the very least, this includes the server, but many offices add the doctor's computer, office manager's computer, etc. If it has a patient name, chart ID, date of birth, phone number, or any of 14 other identifiers, then it's ePHI and must be encrypted and backed up. Fortunately, pretty much any computer built in the past 8 to 9 years already has a free encryption program, BitLocker, which is built right into Windows.

5. EMAIL ENCRYPTION

Speaking of encryption, you also must encrypt your online communications with patients and referring offices. Most of the better solutions will work with your existing email address, and you shouldn't have to pay more than $40 to $50 per month for a good, encrypted email system.

6. NETWORK SECURITY

Invest in a business-class firewall. A firewall keeps the bad guys (malware) from entering your network. Stay away from consumer-level devices, such as Linksys and Netgear and TP Link. Instead, consider a firewall from companies like Sonicwall or Fortinet.

7. ANTIVIRUS PROTECTION

Firewalls are a great start, but they are not infallible, so you should have good antivirus software in place. Bitdefender, Emsisoft, ESET, and Trend Micro—there are numerous good antivirus programs.

8. RANSOMWARE

Although most antivirus programs say they are effective against ransomware, that isn't always the case. Consider anti-ransomware-specific software, such as Intercept X or HitmanPro.

9. WHITELISTING

With many viruses being zero-day—meaning they are so new that your software won't recognize them as a virus—you must consider using application whitelisting. Basically, all your good programs that are on the list can run, and any that aren't on the list, such as viruses, get stopped in their tracks.

10. TRAINING

Finally, invest in annual training for you and your staff to stay on top of these security risks.

If your office follows all these top 10 items, you'll be ahead of the game when it comes to meeting HIPAA laws and cybersecurity best practices.

If you need help or have any questions regarding any of these topics,
please call us at 888—388-2774

323 TECHNOLOGIES, INC.
Your Dental IT Partner
1560 E Southlake Blvd. Southlake, TX 76092
http://www.323techs.com
support@323techs.com