Is Your Data Safe? 5 tips for data security in your dental practice…

1. Are you emailing patient information and digital x-rays to other doctors? Make sure that your office and the receiving office utilize encrypted email services. If you don't, your data can easily be read on its path from your practice to theirs. HIPAA states that you are responsible for making a reasonable attempt at protecting your data.

2. Do you have a wireless router in your office? If you are using wireless Internet for internal purposes, make sure your router is a current model with the latest security standards. Most wireless routers (especially those purchased from retail outlets) do not default to their most secure settings, making them susceptible even for entry-level hackers. Do you want to be a HOT SPOT and provide free Internet to waiting patients? Make sure your wireless router is segmented (isolated) from your primary network.

3. It is very important to lock down access to your computers at the end of the day. At the very least, you should log out of your practice management software on all workstations to prevent someone who has access to the office (cleaning people, landlord, or intruder) from easily accessing patient files.
An even better method is to password-protect and completely log off your computer at the end of the day, which will prevent access to documents that are stored outside your practice management software. These are very simple processes to implement.

4. Are you backing up your data properly? In more cases than not, the tapes you are swapping or the portable hard drives you are lugging around are not enough. Tapes can wear out and sometimes do not correctly back up your data. If you are using tapes, then you should regularly conduct test restores to assure that the data you need is being backed up. Portable hard drives, while cheap and easy, can result in the same problems as tapes. Make sure you conduct test restores. In addition, most backups to portable hard drives are not encrypted. This means anyone who plugs in your drive can steal your data.

There are many options available today. There are a lot of good remote backup solutions that use the Internet, but encrypt the data so it is protected. Also, there are new disaster recovery systems that back up data to a local storage device as well as a remote location. Make sure your backups happen regularly and that whatever you back up to is in a safe place outside your office. You can never back up too often or too securely.

5. Is your practice anti-virus and anti-malware software current? It is very important that every computer in your practice is protected by current anti-virus and anti-malware software. It significantly decreases the likelihood of a malicious infection. Unfortunately, it is not 100% foolproof, as users can still bypass threat warnings to access something they think they need. In addition to the software with an active update subscription, your staff needs to be educated on what websites to go to and not to go to. A firewall with built-in anti-virus software and filtering can further enhance security and protect from operator error.

It is well worth the effort to make sure that your practice's data is secure and protected. After all, your practice data is a good portion of your business. What would you do without it?

Tom Terronez is president of Medix Dental, a dental technology consulting company that provides dental practices the technical expertise, resourcefulness and solutions that will increase productivity and make their practice the best practice they can be. For more information, visit www.medixdental.com.

Medix Dental
220 N Main Street, Suite 410
Davenport, IA 52801
877.885.1010 **toll free**
563.355.7300 **local**
563.322.4500 **fax**