How to Ensure Patient Medical Data is Safe

This is an extra resource to go along with the original article:
3 privacy concerns for electronic forms and records

Keeping patient data safe is essential to the well being of your practice as well as the well being of the patients themselves. Here are five steps to ensuring that your patient medical data remains as secure as possible.

1. Educate Staff and Patients

Educating staff and patients about the best line of defenses against data theft can help mitigate the damage of potential threats. Employees should be informed about any privacy policies and security measures you and your EMR/EHR provider has in place, and only authorized users should have access to patient data. It's also important to educate patients who may access their personal records using a Patient Portal.

2. Limit Access from Mobile Devices

Patient data may often be stored or accessed from mobile devices from outside of the office, which means that patient data may be more vulnerable to attack. Protecting devices such as laptops, smartphones, and tablets with encryption and passwords is another way to avoid a potential data breach. You should also remind employees never to leave their mobile devices unattended. If mobile devices used to access patient information are stolen or missing, passwords and security codes should be changed.

3. Double Check Email Addresses and Beware of Phishing Scams

Email can be a problematic source for data breaches. Emails accidentally sent to the wrong address can release personal patient medical information to the wrong party, with potentially devastating results. Make sure that emails in your system are updated and correct, and double check them before sending private data over email. You should also be aware of patient information being solicited through email, also known as "phishing." Instruct staff not to open any emails that are unfamiliar and to get confirmation from an email user who requests personal information over email.

4. Keep Software and Anti-Virus/Anti-Malware Up to Date

While your EMR/EHR service provider should be keeping their systems up to date, oftentimes practitioners or office staff will fail to update their own systems, even when alerted. For the sake of patient privacy and to prevent security breaches to the best of your ability, it's essential that software is updated immediately when new versions are released. If you're unsure whether or not your software is out of date, contact your EMR/EHR provider to double check.

5. Secure Your Network and Wireless Internet Passwords

It's important to make sure your network passwords are secure (they should be complex passwords that are not easy to guess, for one) and that only authorized individuals have those passwords. It's good to remind authorized individuals never to store their passwords in visible places, like on notes or paper at the front desk, or in a text file on a publicly shared computer, for example. Employees should never give out passwords to unauthorized users, and passwords should be changed if there is a potential threat, like a missing device or suspicious activity.