EMR Safety Checklist for Healthcare Providers

This is an extra resource to go along with the original article:
How safe are your electronic medical records?

To ensure that your Electronic Medical Records (EMR) are as secure as possible, make sure that your healthcare office, clinic or hospital can check off these important safety measures.

1. Our files have bank-level security encryption

Bank-level security encryption scrambles information when it is transmitted over the internet using a cypher (i.e., an encryption algorithm)—like a 256-bit or better Secure Socket Layer (SSL)—and a cipher key. Data transmitted over an SSL connection can't be tampered with or forged without the two parties becoming immediately aware of the tampering, which means that if an attack occurs, you'll be notified. If you're not sure whether your EMRs have this, contact your EMR vendor or security manager.

2. We have established secure password guidelines

Your EMR system should have strict password guidelines to better protect your patient data. Look for a TRUSTe Certified Privacy badge on your EMR vendor's website, or contact your vendor to double check. To earn the privilege of displaying that badge, the EMR must employ strict password guidelines and feature unique password-protected access. Clinic computers should also have strict password guidelines established by your own team when creating logins for staff, nurses and practitioners.

3. We perform regular automatic data backups

Your EMR system should already perform automatic backups, but you may have to double check that this feature is active. You should also ask your EMR vendor if backups additionally stored offline in case of an attack or a system failure that results in the loss of online records.

4. Our EMR system has an audit trail (and it's turned on)

An audit trail monitors user activity, which discourages hackers from using it for fraud. So long as providers keep the feature turned on, the audit trail will maintain a chronological record of all attempts to access patient files. It records the data accessed, who accessed it, and when and from where it was accessed.