Top 10

Security Tips to Keep You and Your Patients Safe

1 Log Out of EHR Systems When You're Done

Don’t leave patient records open. Log out every time you step away, even for a minute.

2 Don’t Share Your Username or Password (Ever)

Everyone needs their own login. Sharing breaks HIPAA rules and audit trails.

3 Use Approved Messaging Tools for Patient Info

No texting PHI through your phone or using unapproved apps. Use your office’s secure system.

4 Check Emails from Labs & Insurers Before Clicking

Emails that look like they’re from labs, insurers, or leadership might be phishing. Ask IT if you're unsure.

5 Keep Screens Away From Public View

Turn monitors away from waiting rooms and use privacy screens if needed.

6 Shred Printed PHI When You’re Done

No throwing papers with patient names in the trash. Shred them.

7 Encrypt Laptops and Mobile Devices

Lost devices = data breaches. Always use passwords and encryption if you access patient info.

8 Don’t Talk About Patients in Public Areas

Hallways, elevators, and cafeterias aren’t private. Save it for behind closed doors.

9 Report Anything Suspicious Immediately

If you see a weird pop-up, a stranger in a restricted area, or an email that seems off—tell IT or your supervisor.

10 Follow the “Minimum Necessary” Rule

Only access or share the patient info you need for your job—nothing more.

Learn more at
phinsecurity.com