Healthcare Security TOP 10 Critical Measures to Safeguard Patients and Data

01

Always Log Out of EHR Systems When Done

Never leave patient records accessible when stepping away, even briefly.

02

Never Share Your Credentials

Individual logins protect compliance and audit trails; do not share usernames or passwords.

03

Use Approved Secure Messaging Tools for PHI

Protect patient health information by avoiding unapproved apps or texting.

04

Verify Emails from Labs and Insurers Before Clicking

Confirm suspicious emails through IT before taking any action.

05

Position Screens to Prevent Public Viewing

Use privacy screens and direct monitors away from waiting areas.

06

Shred Printed PHI Promptly

Destroy all paper documents containing patient data securely—never discard openly.

07

Encrypt All Laptops and Mobile Devices

Always protect devices with passwords and encryption to prevent data breaches.

08

Avoid Patient Discussions in Public Spaces

Keep sensitive conversations confined to private environments.

09

Report Suspicious Activities Immediately

Alert IT or supervisors about unusual pop-ups, unauthorized personnel, or questionable emails.

10

Follow the Minimum Necessary Principle

Access and share only the patient information essential for your role.

vyings

Contact **VYINGS** for fractional cybersecurity leadership.

www.vyings.com

info@vyings.com

Need help securing your organization?