HIPAA & Cybersecurity Quick Tip Sheet

HIPAA COMPLIANCE

1. Core HIPAA Principles

- **Privacy Rule:** Protect patient information (PHI) in all forms—verbal, written, and electronic.
- **Security Rule:** Safeguard electronic PHI (ePHI) through administrative, physical, and technical measures.
- **Minimum Necessary Standard:** Access or share only the information needed to perform your job.
- **Patient Rights:** Patients can request access to their medical records and must authorize most disclosures.
- **Reporting:** Immediately report any suspected privacy or security incident to your Privacy or Security Officer.

2. Everyday HIPAA Best Practices

- Never discuss patient information in public or common areas.
- Always **lock your computer screen** when leaving your desk.
- Verify fax numbers and email addresses before sending PHI.
- Use **secure messaging or encrypted email** when sharing PHI electronically.
- Store paper charts or printed PHI in **secure areas** when not in use.
- Dispose of PHI only in approved shredding bins.
- Keep **passwords private**—never share them, even with coworkers or IT staff.

3. Cybersecurity Essentials

- **Phishing Awareness:** Don’t click suspicious links or open unexpected attachments. When in doubt, verify with IT.
- **Strong Passwords:** Use strong mix of upper/lowercase letters, numbers, and symbols.
- **Multi-Factor Authentication (MFA):** Always enable it when available.
- **System Updates:** Allow automatic updates and restarts to patch vulnerabilities.
- **Email Security:** PHI must only be sent through secure, HIPAA-approved systems.
- **Device Safety:** Never use personal USB drives/devices for clinic data.
- **Wi-Fi:** Connect only to clinic-approved, secure networks.
- **Data Backup:** Follow your clinic’s backup and recovery protocols.

“What’s one thing we can each do this week to improve data security in our clinic?”

4. What To Do If Something Happens

- If you suspect a **breach**, **ransomware attack**, **lost/stolen device**, or **misdirected email**, report it **immediately** to your HIPAA Privacy/Security Officer or IT department for mitigation.
- Quick reporting helps reduce potential exposure and legal risk.

5. Remember

Protecting patient data is not just compliance—it’s patient trust. Every employee plays a role in maintaining privacy and security every day.