BYOD - VPN / VMware

Applies to: Anyone using a *personal phone, tablet, or laptop* to access hospital email, clinical apps, or systems through VPN.

---

1. Before You Use Your Device

Your personal device **must**:

- Have a **screen lock** (PIN, password, or biometric).
- Auto-lock after **5–10 minutes** of inactivity.
- Use **built-in encryption** (iOS/Android encryption, FileVault, BitLocker).
- Be on a **supported, up-to-date OS** (install updates regularly).
- **Not** be rooted or jailbroken.
- Have **antivirus** installed if it's a laptop.

If it doesn't meet these, it **cannot** be used for hospital access.

---

2. VPN Access Rules

When using VPN from your own device:

- Log in with your **hospital username + strong password + MFA**.
- Only access systems you actually need for your job.
- VPN will **disconnect after inactivity** — log back in as needed.

- Log out and disconnect VPN when you're done working.

---

3. PHI & Data Handling

On personal devices:

- **Do not save PHI** (patient info) directly on your device.
- **Do not sync PHI** to personal cloud services (iCloud, Google Drive, Dropbox, etc.).
- Only access PHI through **approved hospital apps/portals**.
- Do **not** use the regular phone camera for patients or charts (only use an approved secure clinical app if authorized).

---

4. Lost, Stolen, or Compromised Device

If a device used for VPN/PHI access is:

- **Lost**
- **Stolen**
- **Infected with malware** or acting suspicious

You must:

- **Report it to IT/Security immediately.**
- Stop using it for hospital work until cleared.

IT may disable VPN access and remotely wipe hospital data if needed.

---

5. Your Responsibilities

By using your own device for hospital work, you agree to:

- Keep your device **secured and updated**.
- **Never share** your password or MFA codes.
- **Protect PHI** at all times and follow HIPAA rules.
- Only use your **own account** (no shared/family logins).
- Report **suspicious activity or possible PHI exposure** right away.

Remember:
Your device is personal. The data you access is **not**.
Treat patient information like it's yours — and guard it the same way.