Bring Your Own Device (BYOD) & VPN Access Policy

1. Purpose

This policy establishes the security and compliance requirements for employees using personal devices to access hospital systems, email, and clinical applications through VPN. The goal is to protect patient information (PHI), ensure regulatory compliance (HIPAA), and reduce organizational risk associated with BYOD usage.

2. Scope

This policy applies to all staff, contractors, and authorized users who use their personal phones, tablets, or laptops to access hospital networks or systems via VPN or VMware.

3. Policy Details

3.1 Personal Device Requirements

• Devices must have screen lock (PIN, password, or biometric authentication).

• Auto-lock should activate after 5–10 minutes of inactivity.

• Devices must use built-in encryption (e.g., iOS/Android encryption, FileVault, BitLocker).

• Operating systems must be supported and regularly updated.

• Devices must not be jailbroken or rooted.

• Laptops must have antivirus software installed.

3.2 VPN Access Rules

• Users must authenticate with a hospital username, strong password, and multi-factor authentication (MFA).

• Access should be limited to systems necessary for job functions (principle of least privilege).

• VPN sessions will time out after inactivity and require re-authentication.

• Users must log out and disconnect VPN after completing work.

3.3 PHI & Data Handling

• Do not store PHI directly on personal devices.

• Do not sync PHI to personal cloud services (e.g., iCloud, Google Drive, Dropbox).

• Access PHI only through approved hospital portals or apps.

• Do not use standard phone cameras for clinical use; use approved secure clinical apps if authorized.

3.4 Lost, Stolen, or Compromised Devices

• Report immediately to IT/Security.

• Cease using the device for hospital work until cleared by IT.

• IT may disable VPN access or remotely wipe hospital data if risk is confirmed.

3.5 User Responsibilities

• Keep the device secure and updated.

• Do not share passwords or MFA codes.

• Protect PHI and follow all HIPAA compliance rules.

• Only use personal accounts — do not share logins with others.

• Report suspicious activity or PHI exposure immediately.

4. Reminder

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