Bring Your Own Device (BYOD)

PURPOSE

To provide principles and guidelines for the secure use of personally owned devices (BYOD) by workforce members when accessing or handling electronic Protected Health Information (ePHI) on behalf of 00BK Healthcare Management LLC ("Organization").

SCOPE

This policy applies to all employees, contractors, and workforce members who use personally owned devices (e.g., smartphones, tablets, laptops, desktops) to access, store, transmit, or process ePHI or any sensitive or protected information belonging to the Organization.

POLICY

The Organization permits the use of personal devices for business purposes only if such use complies with the standards outlined in this policy. Personally owned devices used to access ePHI or sensitive systems must implement and maintain appropriate administrative, physical, and technical safeguards.

BYOD SECURITY REQUIREMENTS

Workforce members using personal devices must adhere to the following security controls:

1. **Authentication and Locking**
    - Devices must be protected with a strong password, passcode, or biometric authentication.
    - Devices must auto-lock after a maximum of 15 minutes of inactivity.
2. **Software and System Updates**
    - Devices must run up-to-date operating systems and install security patches promptly.
3. **Antivirus and Endpoint Protection**
    - Devices must have active antivirus or endpoint protection software installed and maintained.
4. **Encryption**
    - Devices must support full-disk encryption.

    - Any storage of ePHI on a BYOD device must be encrypted using FIPS 140-2 compliant encryption.
5. **Multi-Factor Authentication (MFA)**
    - MFA is required for accessing any systems that store, transmit, or process ePHI.
6. **Prohibited Configurations and Activities**
    - Use of jailbroken or rooted devices is strictly prohibited.
    - ePHI must not be transferred to or stored in personal cloud services (e.g., iCloud, Dropbox, Google Drive).
    - Sharing of personal devices used for work purposes is not allowed.
    - Public Wi-Fi access without a secure VPN connection is not permitted.
7. **Permitted Access Methods**
        - Access to ePHI is permitted only via Approved TLS-encrypted web portals or secure mobile applications

---

INCIDENT REPORTING AND BREACH RESPONSE

- Any loss, theft, or compromise of a personal device used for work must be reported immediately to the Security Official.
- The Organization will follow its Data Security Policy – Incident Response and Reporting procedure.
- The Organization may invoke remote wipe procedures for devices that have been compromised, when feasible.

ACKNOWLEDGMENT AND COMPLIANCE

- Workforce members must complete HIPAA Security Awareness Training before using personal devices for work purposes.
- Workforce members must sign a BYOD Acknowledgment Form affirming their understanding and compliance with this policy.

REVIEW AND REVISION

This policy shall be reviewed annually by the Security Official or when there is a significant change in device usage, applicable regulations, or risk environment. Updates shall be documented and retained.

RELATED POLICIES AND PROCEDURES

- Data Security Policy – Access Control
- Data Security Policy – Information Access Management
- Data Security Policy – Incident Response and Reporting
- HIPAA Security Rule Basics

RELEVANT HIPAA REGULATIONS

- 45 CFR §164.308(a)(3) Workforce Security
- 45 CFR §164.312(a)(1) Access Control
- 45 CFR §164.312(d) Person or Entity Authentication
- 45 CFR §164.310(d)(2)(i)-(iv) Device and Media Controls
