CyberHealth Solutions – Device Access Policy
Version: 1.0
Last Updated: 22/04/2025

1. Purpose
To establish guidelines for secure access and usage of electronic devices that store, access, or transmit protected health information (PHI).

2. Scope
This policy applies to all employees, contractors, and consultants who use devices for work-related purposes.

3. Device Types Covered

- Laptops
- Desktops
- Smartphones/Tablets
- USB Drives & External Storage
- IoT Devices used in clinical settings

4. Policy Guidelines

- All devices must be password protected with strong authentication.
- Devices must auto-lock after 5 minutes of inactivity.
- Remote wipe must be enabled on mobile devices with PHI access.
- No personal device can access PHI unless enrolled in the organization's Mobile Device Management (MDM) solution.
- USB drives must be encrypted; unapproved devices are prohibited.
- Lost/stolen devices must be reported within 24 hours.
- Anti-virus and firewall software must be enabled and regularly updated.

5. Enforcement
Violations of this policy may result in disciplinary action, including termination.

6. Review
This policy will be reviewed annually or as needed.