#

# Bring Your Own Device Policy

#

This office is committed to the protection of PHI available on portable/mobile devices whether used in the office or remotely. All workers (including volunteers, interns, and temporary workers) are required to adhere to this Policy when using a personal Device (such as a laptop, phone, tablet, etc.) for purposes related to office business. The use of these Devices utilizes wireless and sometimes remote access to the office’s network or other applications that contain PHI.

Workers will be given access to only that PHI that is needed to complete his/her role and assigned tasks. Access to PHI is to be granted/revoked in accordance with the *Access Control Policy* and *Workforce Onboarding and Termination Checklist & Audit* located in this Manual. Certain workers may only use portable and mobile computing Devices owned by them for work related tasks inside of the office or while traveling or at home if approved. Workers must contact the Security Officer and/or IT Support PRIOR to using a Device owned by them and PRIOR to providing an approved Device to a third party for repair or exchange (e.g. wireless phone provider) so precautions can be taken to protect or remove PHI and other office information. Violations of this policy will be addressed in accordance with the *Sanctions Policy*.

If the office’s IT Support is a third-party company/individual, the BAA must require this policy be followed for this office’s workers.

**Requirements for Approving an Employee-Owned Portable Device:**

All worker-owned Devices must:

* + Be approved by the Security Officer and accounted for on the office’s computer asset inventory.
	+ Use the same security controls as described in the Technical Safeguards section of the Security Plan in this Manual prior to use.
	+ Use the additional controls selected below. A checklist to this policy to complete for each Device and with each worker.

Device Configuration.

Check the boxes next to each requirement this office requires for employee-owned Devices:

* Device syncs with the office’s network.
* Device files are saved on the server and part of the routine backup.
* PHI cannot be saved on the Device’s hard drive.
* All Devices are to be encrypted. Encryption keys are kept separate from the Device by the Security Officer or their designee.
* Screenshot functionality will be disabled, if possible, on Devices with access to PHI.
* If not disabling screenshot functionality is not possible, workers are trained about the risks related to taking and saving screenshots.
* Malware protection must be enabled on all Devices along with automatic live updates/patches.
* If a security patch or update is not able to be downloaded by the worker, the Security Officer will notify, by email, all workers with Devices with instructions on how to download and install the update.
* A confirmation of the email and notification of the update will be kept as well as evidence of installation of the update.
* The Security Officer is permitted to take possession of the Device to ensure updates.
* Device is configured with security controls that will remotely wipe the Device upon loss or theft, scan for malware, provide Global Position System (GPS) tracking.
* Devices that are used to access, receive or transmit PHI shall be configured to limit the amount number of emails, text messages or other instant messages stored on the Device. Only secure messaging systems approved by the Privacy and/or Security Officer are permitted.
* Workers are prohibited from connecting to unsecured, public wi-fi networks (wi-fi access that does not require a password to use and/or owned by a third-party like a coffee shop or airport). All workers will be trained and sent periodic reminders to only pair their Devices with approved systems, networks, or other devices while in a private location, ideally the office or at home.
* Workers will not be able to change any setting or security rule on a Device. Any changes to settings related to security must be performed, recorded, and tracked by the Security Officer.
* Flash drives and other media copying capabilities should be disabled. If not possible, appropriate training, encryption, and monitoring will be implemented.
* Devices may be “wiped” or erased, and subject to inspection without prior notice for privacy and security purposes

|  |
| --- |
| Each worker must read this policy and sign the *BYOD Form* (attached) prior to using a Device not owned by this office for office business. |

#

# Bring Your Own Device Form

#

Use this form for any worker-owed Device to be approved for office use as described in the *Bring Your Own Device* policy in the *Employee Policies* section of this Manual.

Type of Device: .

Device configuration matches the requirements in the *Bring Your Own Device* policy.

🗆 Yes

🗆 No

If no, explain:

Configured or reviewed by IT/Security:

|  |
| --- |
| I, , have read the *Bring Your Own Device* policy Employee Printed Name |
| and will adhere to its requirements. I understand that if I bring my own device to use for the office’s business purposes, it will be subject to the requirements listed in the policy. |
| Employee Signature: Date:  |