#

# Work From Home/Remote Access Policy

#

This office is committed to offering workers (including volunteers, interns, and temporary workers) flexible working conditions, where roles and responsibilities permit. This office is also committed to the protection of PHI available via a remote network connection or via cloud-based applications. All workers are required to adhere to the following when accessing the office’s network and cloud-based systems containing PHI.

Workers will be given access by the office only to that PHI needed to complete assigned tasks in accordance with the *Access Control Policy* and *Workforce Onboarding and Termination Checklist* in this Manual. Any Device (laptop, tablet, smartphone, etc.) to be used to remotely access the office’s network and PHI must be issued or approved by the office’s Security Officer and/or IT Support and in accordance with the office’s *Bring Your Own Device Policy* in this Manual, as applicable. Violations of this policy will be addressed in accordance with the *Sanctions Policy* in this Manual.

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.

**Process**:

1. All Devices owned, issued, or approved for worker access to the office’s network or cloud-based applications containing PHI must be:
	* Approved by the Security Officer and/or IT Support; and
	* Accounted for on the office’s computer and software asset inventory.
2. The office’s IT Support must configure/approve the Device’s security controls and the user’s access credentials in accordance with the office’spolicies regarding Technical Safeguards in this Manual.
3. Prior to receiving permission to access the office’s network remotely, each user must:
	* Read, understand, and acknowledge:
		1. this Policy. See below;
		2. the *Bring Your Own Device* policy in this Manual, if applicable;
		3. the remote workspace physical security requirements required by this Policy;
	* If the user is a third-party vendor, verify that a business associate agreement is in place with the office prior to granting access to the office network and PHI.
4. Check the box next to each remote workspace physical security requirement required by this office. The office reserves the right to periodically request reevaluation and acknowledgement of these requirements and may revoke access if it is reasonably believed that one or more of these safeguards are not in place.
* Remote work is to be performed in a room/office unused by others during working hours
* Worker must use private areas for phone conversations
* Fire safety equipment (detector/extinguisher) is to be present and functional in the work area
* Privacy screen for monitor/Device(s) must be used
* Device(s) must be stored in a secure location or carried with worker at all times when not in use
* External media (USB, CDROM, etc.) will not be used
* May be “wiped” or erased, and subject to inspection without prior notice for privacy and security purposes
* Other:

#

# Work From Home/Remote Access Form

#

Use this form for any worker who will have remote access to the office network or systems containing PHI.

As a condition of working remotely while connected to this office’s network or accessing cloud-based applications containing PHI, the physical safeguards required in the *Work From Home/Remote Access* policy in the *Employee Policies* section of this Manual must be in place for any remote workspace(s) used by the worker. This office reserves the right to periodically request reevaluation and acknowledgement of these requirements and may revoke access if it is reasonably believed that one or more of the required safeguards are not in place.

Type/location of access: .

|  |
| --- |
| I, , have read this *Work From Home/Remote Access* policy and Printed Name |
| procedure and will adhere to its requirements including the required physical safeguards. I understand that if I bring my own device to use for the office’s business purposes, it will be subject to the requirements in the *Work From Home/Remote Access* policy and the *Bring Your Own Device* policy.  |
| Signature: Position/Role: Date:  |