Work From Home/Remote Access Policy

This business is committed to offering workers (including volunteers, interns, and temporary workers) flexible working conditions, where roles and responsibilities permit. This business 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 business's network and cloud-based systems containing PHI.

Workers will be given access by the business 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 business's network and PHI must be issued or approved by the business's Security Officer and/or IT Support and in accordance with the business'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 business's Security Officer/IT Support is a third-party company/individual, the written agreement between the business and IT Support company/individual must require adherence to this policy. The term Security Officer, as used in this policy, includes an business employee or a third-party.

Process:

1. All Devices owned, issued, or approved for worker access to the business's network or cloud-based applications containing PHI must be:
    - Approved by the Security Officer and/or IT Support; and
    - Accounted for on the business's computer and software asset inventory.
2. The business's IT Support must configure/approve the Device's security controls and the user's access credentials in accordance with the business's policies regarding Technical Safeguards in this Manual.
3. Prior to receiving permission to access the business's network remotely, each user must:
    - ☐ Read, understand, and acknowledge this Policy by signing below;
    - ☐ Acknowledge the *Portable Device or Bring Your Own Device Policy* in this Manual;
    - ☐ Read and understand the physical security requirements attached to this policy;
    - ☐ If the user is a third-party vendor, verify that a business associate agreement is in place with the business prior to granting access to PHI

Employee Acknowledgement on Following Page

PHYSICAL SECURITY SAFEGUARD REQUIREMENTS FOR REMOTE WORK/ACCESS TO THE BUSINESS'S NETWORK

As a condition of working remotely while connected to this business's network or accessing cloud-based applications with PHI, the physical safeguards checked below must be in place for any workspace(s) used by the user. The business 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 performed in a room/office unused by others during working hours
- ☐ Use of private area for phone conversations
- ☐ Fire safety equipment (detector/extinguisher) is present and functional in the work area
- ☐ Privacy screen for monitor/Device(s)
- ☐ Device(s) stored in a secure location or carried with user at all times when not in use
- ☐ External media (USB, CDROM, etc.) will not be used
- ☐ Other: _____

I, _____, have read this *Work From Home/Remote Access Policy* and
Printed Name

procedure and will adhere to its requirements including the physical safeguards listed below. I understand that, if I bring my own device to use for business purposes, it will be subject to the requirements listed above and the *Bring Your Own Device Policy* and may be "wiped" or erased, and subject to inspection without prior notice for privacy and security purposes.

Signature: _____

Position/Role: _____

Date: _____