
# Telecommuting Audit and Policy

HIPAA SEAL OF COMPLIANCE
HIPAA VERIFIED

Compliancy Group

## Objective of Telecommuting:

Telecommuting allows employees to work remotely at home for a part of their regular workweek. Telecommuting is a voluntary work alternative that may be appropriate for some employees and some jobs.

## Requirements of HIPAA Compliance for Telecommuting with Employee Managed Equipment:

- The employee must have a device that the employee will dedicate for business purposes only.
- The employee must ensure the device drives are encrypted – this can be accomplished by using an encryption application like Microsoft BitLocker (requires Windows 10 Pro) or Apple FileVault.
- The employee must install Anti-Virus and Malware Protections.
- The employee must turn on Automatic Updates.
- The employee must have a strong password protected account on the computer.
- The employee must use a strong password that is at least 12 characters or more with an uppercase letter, a lowercase letter, a number and a symbol – this password does not need to be changed unless there is suspicion that the password has been compromised.
- The employee must have a password protected screen lock timeout set to a maximum of 15 minutes.

# Requirements of HIPAA Compliance for all Telecommuters:

- The employee must make sure wireless router traffic is encrypted using (at a minimum) WPA2-AES encryption.
- The employee must make sure that the password to the wireless network is a strong password that is at least 12 characters or more with an uppercase letter, a lowercase letter, a number and a symbol.
- The employee must never download or print PHI – no footprint (evidence of PHI) will be allowed at Home Offices.
- The employee must conduct the physical site audit (end of this document) and provide the details of the audit to the current Security Officer every 12 months.
- If the above are not followed, the employee must defend their decisions to the Department of Health and Human Services (HHS) should a breach occur, and it be revealed that these protocols were not followed.
- Have a member of the organization's IT department confirm all requirements are in place before access to company resources is granted.

# Home Office Site Audit

| Questions completed by Employee: | Yes | No | N/A | Notes |
|---|---|---|---|---|
| Do you store paper documents that contain Protected Health Information in your home office? | | | | |
| Do you print paper documents that contain Protected Health Information at your home office? | | | | |
| Do you receive paper faxes at a physical fax machine in your home office? | | | | |
| Do you take paper or electronic files containing Protected Health Information to your home office? | | | | |
| Do you have a lockable door to your home office? | | | | |
| Do you have an alarm on your home / home office? | | | | |
| **Questions completed by the IT Department:** | **Yes** | **No** | **N/A** | **Notes** |
| Is the drive on the computer encrypted using either Apple FileVault or Microsoft BitLocker encryption? | | | | |
| Does the computer have an Anti-Virus and Malware Software installed? | | | | |
| Are automatic updates turned on? | | | | |
| Is the computer password protected with at least a 12-character complex password? | | | | |
| Is the computer set to lock after a maximum of 15 minutes of inactivity on the computer? | | | | |
| Does the employee have a Wireless Router? | | | | |
| If they have a Wireless Router is it protected using WPA2-AES and a strong password? | | | | |

**Signed and Agreed to by:**

Employee Signature: _____ Date: _____

Print Name: _____ Title: _____

Supervisor Signature: _____ Date: _____

Print Name: _____ Title: _____