**MEMORANDUM**

To: PLPC Clients

From: Margaret E. Long

Date: March 24, 2020

Re: HIPAA Issues While Telecommuting

In light of COVID-19, it is anticipated that employees will have to provide essential services at home. HIPAA privacy and security rules do not prohibit remote access, but they do require that organizations implement appropriate safeguards to ensure the privacy and security of protected health information (PHI). It is recommended that the following safeguards be put in place to protect the PHI.

*IT Requirements*:

* Make sure that all devices accessing your network are properly configured by IT. Devices must be encrypted, password protected, and installed with software firewalls and anti-virus software installed.
* Require that employees use a VPN when they access the company’s Intranet remotely.
* All PHI must be encrypted before being transmitted. This can either be through the company’s Intranet or using the internal email encryption.
* Require that any personal devices employees use to access PHI are to be Encrypt and password protected.

*Security and Privacy Requirements*:

* Employees should not allow any friends, family, etc. to use devices that contain PHI.
* Employees should not allow any friends, family, etc. in the room when they are accessing records that contain PHI.
* Have each employee sign a Confidentiality Agreement to assure the utmost privacy when handling PHI.
* Employees should be prohibited from using their own equipment.
* Employees should be instructed not to store hard copies of PHI. IF they need to store PHI in their home office, they need to store it in a lockable file cabinet or safe to store the information.
* Make sure employees disconnect from the company network when they are done working. Usually, IT configuring timeouts take care of this.
* Employees cannot copy any PHI to external media not approved by the company. This includes flash drives and hard drives. You may require all PHI to stay on the company network.
* Keep logs of remote access activity, and review them periodically. IT should disable any accounts inactive for more than 30 days.
* Mandate that any employees in violation of these procedures will be subject to Discipline.