HIPAA Confidentiality and Non-Disclosure Agreement

I, _____ (Your Name), do affirm that I will not divulge The INFORMATION TO ANY UNAUTHORIZED PERSON FOR ANY REASON. Neither will I directly nor indirectly use, or allow the use of, information for any purpose other than that directly associated with my official assigned duties. I understand that ALL INDIVIDUALLY IDENTIABLE INFORMATION, including financial data, is strictly confidential.

Furthermore, I will not, either by direct action or by counsel, discuss, recommend, or suggest to any unauthorized person the nature or content of any individually identifiable information.

I will not, either by direct action or by counsel, discuss, recommend, or suggest to any unauthorized person the nature or content of any individually identifiable information.

I agree to adhere to Office Policies and Procedures. In addition to compliance with all other Security Policies and Procedures, I agree not to:

- **Crashing an information system**. Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred as a result of user action, a repetition of the action by that user may be viewed as a deliberate act.

- **Attempting to break into an information resource or to bypass a security feature**. This includes running password-cracking programs or sniffer programs, or attempting to circumvent file or other resource permissions.

- **Introducing, or attempting to introduce, computer viruses**, Trojan horses, peer-to-peer (“P2P”) or other malicious code into an information system. Exception: Authorized information system support personnel, or others authorized by the Office Security Officer, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.

- **Browsing**. The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. The Office has access to patient health information which is protected by HIPAA regulations which stipulate a "need to know" before approval is granted to view the information. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.

- **Personal or Unauthorized Software**. Use of personal software is prohibited. All software installed on Office computers must be approved by the Office.

- **Software Use**. Violating or attempting to violate the terms of use or license agreement of any software product used by the Office is strictly prohibited.

- **System Use**. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of the Office is strictly prohibited.

Remote access to company's network systems is permitted using the company's private virtual private network (VPN) or GoToMyPC.com as authorized by my Office's Security Officer

The emailing of individually identifiable information may only be done using company email accounts and in accordance with the Office's Security Policies. No individually identifiable information may be included in the subject line or body of an email transmission. Company email accounts transmit and receive emails using secure socket layer (SSL) connections.

I understand and acknowledge the disciplinary action up to and including termination of my employment, position, contractual relationship, whichever applicable, may result from the following privacy and security violation:

Level 1 **Description of Violation**

- Accessing information that you do not need to know to do your job.
- Sharing computer access codes (user name & password).
- Leaving computer unattended while being able to access sensitive information.
- Disclosing sensitive information to unauthorized persons.
- Copying sensitive information without authorization.
- Changing sensitive information without authorization.
- Discussing sensitive information in a public area or in an area where the public could overhear the conversation.
- Discussing sensitive information with an unauthorized person.
- Failing or refusing to cooperate with the Information Security Officer, Security Officer, Chief Information Officer, and/or authorized designee.

Level 2 **Description of Violation**

- Second occurrence of any Level 1 offense (does not have to be the same offense).
- Unauthorized use or disclosure of sensitive information.
- Using another person's computer access code (user name & password).
- Failing or refusing to comply with a remediation resolution or recommendation.
- Posting or otherwise publishing protected health information on social media or in other venue or channels of distribution.

Level 3 **Description of Violation**

- Third occurrence of any Level 1 offense (does not have to be the same offense).

- Second occurrence of any Level 2 offense (does not have to be the same offense).
- Obtaining sensitive information under false pretenses.
- Using and/or disclosing sensitive information for commercial advantage, personal gain, or malicious harm.

If I am an employee, I recognize that my employment is “at-will” and may terminate at the will with or without cause. Nothing in this Agreement is intended or shall be construed to alter this at-will-employment status and relationship.

I recognize that my files or electronic communications may be reviewed or monitored to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as Office policies.

The failure to insist in my compliance with one (1) or more instances any of the terms or provisions of this Agreement shall not be construed as a waiver or relinquishment for the future of any such term or provision, but the same shall continue in full force and effect.

Once signed, any reproduction of this Agreement made by reliable means (e.g., photocopy, facsimile) is considered an original.

I understand that signing this document does not preclude me from reporting instances of breach of confidentiality.

Signed _____

Name: _____

Date _____