Confidentiality Statement **Form 7.10-Part I**

Through your employment activities and duties, you may learn of, or have access to employee protected health information and protected health information of patients. Protected health information (PHI), for employees and patients, is defined as any information that identifies an individual (patient) and describes their health status, sex, age, ethnicity, or other demographic characteristics, in any format (i.e., electronic, written, or oral). PHI, including financial information, is to be maintained in a confidential manner, and is protected by law and by the privacy policies of this practice. The intent of the laws and policies is to ensure that PHI remains confidential, and is used only to provide for employee or patient care and services.

Your duties, obligations and responsibilities with regard to confidentiality are described below in the form of an agreement with this practice. You are required to abide by these, as well as the Acceptable Use guidelines outlined on the following page. Violations will subject you to discipline, which may include termination of employment, legal liability, and fines imposed by regulatory agencies, depending upon the circumstances.

Confidentiality Agreement - I, the undersigned employee, agree to the following:

1. I will use protected health information only as needed to perform my legitimate duties as an employee of this practice. This means, among other things, that:
   - I will only access protected health information necessary for the performance of my duties;
   - I will not in any way divulge, copy, release, sell, loan, review, alter or destroy any confidential information, except as properly authorized by my employer; and
   - I will not misuse or act carelessly with protected health information.

2. I will safeguard and will not disclose information that could provide access to protected health information by persons outside of this practice.

3. I will report activities by any person or entity that I suspect may compromise the confidentiality of protected health information. (Reports made in good faith about suspect activities will be held in confidence to the extent permitted by law, including the name of the individual reporting the activities.)

4. I understand that my obligations for maintaining confidentiality of protected health information maintained by this practice will continue after termination of my employment.

5. I understand that I have no right or ownership interest in any protected health information referred to in this agreement. My employer may at any time revoke my access to confidential information. At all times during my employment, I will safeguard and retain the confidentiality of all protected health information.

6. I will be responsible for any misuse or wrongful disclosure of confidential information and for my failure to safeguard my means of access to confidential information. I understand that my failure to comply with this agreement may result in legal liability and/or my loss of employment.

_____

Employee Name

_____ _____

Employee Signature Date

Acceptable Use of Communication and Information Systems **Form 7.10-Part II**

Scope – *Acceptable Use* applies to your access and use of communication and information systems, and includes, but is not limited to, proprietary business information, patient information, protected health information, computer hardware, software, email, voice mail, internet, telephone, cell phone, laptops, or other electronic equipment or network service or resources that are owned, leased, used, operated, or provided by the practice.

Communication and information systems of the practice are to be used solely for the conduct of practice business during working hours. Management must approve any type of personal use in advance. Communication and information systems must be used in a responsible manner, and such use must not result in any additional expense to the practice, any possible embarrassment or harm to the practice, any loss in productivity with regard to your work, or any violation of Federal or State regulations. Use of portable media such as zip, flash, or jump drives and/or portable hard drives is expressly prohibited, unless authorized by management.

Responsibilities – It is the responsibility of each person or entity to:

- Protect proprietary information of the practice, such as business practices and financial information, because it is the property of the practice.
- Use or disclose only business or patient information as necessary to perform assigned duties or responsibilities, as deemed necessary by the practice.
- Promptly report the theft, loss or unauthorized disclosure of proprietary or patient information.
- Exercise good judgment in the use of the information system, including internet access and the sites you visit, using caution when opening email attachments, etc.
- Ensure that your use of the practice's information system does not violate any local, state, federal, or international law while utilizing the practice's information system.
- Understand that your use will be monitored as a measure of security, and any data you access, create or transmit is subject to audit, inspection, and review by the practice, whether it is for business purposes or personal use.

Sanctions – You may be subject to disciplinary actions if it has been determined that your use of the practice's information system caused harm, you made unauthorized use or disclosure of proprietary or patient information, or you violated regulatory requirements. Sanctions can include disciplinary actions up to and including termination of employment. Additionally, you could be subject to prosecution and monetary penalties imposed by regulatory agencies.

When in Doubt – Regulatory requirements, technical capabilities of the information system, and operational procedures of your practice are all subject to change. If you are in doubt regarding use or disclosure of proprietary or patient information, ask for assistance or clarification. Asking for assistance will ensure you take the right course of action, and may often be helpful to other members of your practice's team. Remember that fulfilling your responsibilities helps ensure the overall security of your practice's information system and its contents.