**PPC PRIVACY POLICY
Updated October, 2015**

We are required by law to maintain the privacy of your protected health information (PHI). We will only disclose pertinent PHI for essential clinical purposes such as discussions with specialist doctors or hospitals, to convey information to you or your POA, for insurance purposes to obtain payment, or to federal or state agencies when mandated by law. We will use only limited identifying information in the office when we call patients or speak to them about certain items, and we will always assure that such information is kept as limited and confidential as is possible. Any other disclosure of PHI will be done only with your consent. Under all circumstances we will only disclose the minimal amount of PHI that is necessary for the particular purpose for which it is used. We will use every precaution to assure that your PHI is always protected. If we do determine that your PHI has been breached or exposed, we will report that to you immediately.

We typically communicate with patients, doctors, and nurses by email, fax, or phone. We will not include any identifying information in our correspondence other than a patient’s name, and we typically use only part of the name (First name, last initial). Our email is hosted locally and is secure; we utilize every precaution to assure that no one will be able to access our correspondence other than those to who it is directed. If a patient prefers that the practice not convey PHI through a specific means, such as email, such a request can be made to the practice in writing, and other accommodations can be made for communication.

At times we may be asked by family members, physicians, or even friends to disclose medical information about you. We will only send such information if the person requesting such information is a POA, a person you designate as being able to access information, or a physician who you are currently seeing. We will always provide PHI to a hospital or health center if they require that information for clinical purposes. We will also provide information for public health purposes if requested. There are also extenuating circumstances such as subpoenas, law enforcement demands, or even mandates by federal health agencies when we will be asked to provide limited PHI, and in those circumstances we will comply.

All PPC patients have a right to look at or get copies of their PHI upon request. We will always make PHI available through our patient portal, which our patients can voluntarily access at any time, and which is safe and protected. Our patients also have a right to receive a list of any instances when we have disclosed some of your PHI.

If you seek more information about our privacy practices or you have any questions or concerns, you have the right to contact us at any time. If you believe that we have violated your privacy rights or you disagree with a decision we made about disseminating your PHI, you can complain to us or submit a written complaint to the US Department of Health and Human Services.

We do have a vigorous policy to maintain HIPAA. This includes:

**PPC HIPAA Security Program**

* A full security risk analysis is conducted regularly in conjunction with our tech expert, David Dodson, and our EMR software, Prime Clinical. That analysis is part of our meaningful use program. Our computer system is fully secure from breaches and is regularly monitored. We conduct such analyses quarterly, and the computer analyses security is conducted weekly by IT Care. Any security issues are immediately brought to our attention and rectified. None have occurred as of the writing of this updated version of our privacy policy.
* All office workstations are kept out of view of patients, have individual log on codes to both enter the computers and to enter the medical record programs, and are turned off when not being used. No ePHI is kept in the office; we do have old records in the office. The office is locked and people entering the office are required to sign in at the Lorien front desk when the office is closed.
* All portable workstations belong to individual practitioners and workers, have individual log ons both for the computer and the software, and are only used in locations where privacy can be maintained both electronically and physically.
* Our EMR program will shut off if not accessed for several minutes. It is accessed remotely through our server, and requires multiple passwords for entry. Each office employee who has access to the EMR has his/her own passwords. Any employee who leaves the organization has his/her passwords deleted and therefore has no ability to access PHI.
* All employees of PPC have access to all PHI, but we have a minimal necessary policy whereby we only access information that is needed for clinical purposes. All employees also get HIPAA certification annually.
* Our system is connected only to private internet on a secure server monitored by Simple IT and not to public sources.
* Our system has constant security surveillance by our tech team, and we are made aware of any breaches or irregularities through weekly reports. Our system is loaded with all security software.
* Our medical software is not stored on individual workstations but rather on a single server with a backup through a secure company sponsored by our tech expert. Therefore, each individual workstation contains no PHI and thus does not require special policy for disposal or if lost or stolen.
* Our server is in a locked secure server location in Baltimore that has 24 hour surveillance, monitored regularly by IT Care.
* Our backup files are similarly in both the secure server location, and also in an encrypted NAS monitored by IT Care.
* Any security breaches will be tracked and recorded. There are sanctions for security violations including possible monetary fees and even termination of employment.
* Andy Lazris, the owner of PPC, serves as the security officer. He gets more extensive HIPAA certification annually.
* PPC addresses security issues on a regular basis through email correspondence and at our monthly office meetings. Such training is ongoing. During such meetings we regularly evaluate and improve our security preparedness.
* Our electronic communication is done through email that is cloud-based and that is monitored by our tech team. As of this update we are implementing an encrypted email system. Until now we have used only minimal information in our correspondence, and have had no breaches, and use encryption of email through our EMR for more detailed PHI communication. Further information on this aspect of our policy is available in a separate statement. All our email is saved in our secure server that is a locked unit in Baltimore with 24 hour surveillance.
* We send reports through our EMR email system, which is secure and encrypted.
* All our faxes go through our EMR system, which is secure.
* We do conduct email conversations on our portable phone devices. Those conversations are saved through our central cloud storage. We regularly delete any correspondence from both our phones and our computers to assure that minimal PHI will be released in case either device is lost or stolen. We also have no identifying information on our electronic communication beyond names, and we only transmit minimal clinical information that is absolutely necessary for its purpose. We do not communicate with text messaging.

**We ask that all of our patients sign a form to assure that they understand and accept our privacy policy. Such a form is available on our website and can be provided by our front staff.**

HIPPA requires that patient information be kept confidential. Email and phone messages are our primary means of communication and are safe and secure. Please be sure to read our office privacy policy and ask us any questions.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature Date