

## **Standards of Conduct Regarding Privacy**

### **Mission Statement**

**ROBERT A. GADLAGE, M.D., P.C** ("Provider") is committed to conducting its business with integrity and to comply with health care laws, including applicable health information privacy laws, including, but not limited to, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Failure to comply with these laws could result in violations of existing contractual arrangements and, in some circumstances, result in criminal, civil and administrative sanctions to individual employees and Provider. Provider can meet its commitment to compliance only through the efforts of its directors, officers, employees, and independent contractors, each of whom must perform his or her duties on behalf of Provider with honesty and integrity. Although each individual ultimately is responsible for his or her own conduct, Provider is committed to maintaining a working environment that fosters conduct consistent with these ideals regarding the use and disclosure of Protected Health Information.

### **PROVIDER STANDARDS OF CONDUCT**

#### **SCOPE**

Contemporaneously with the adopted of this HIPAA Compliance Plan, Provider has also approved and adopted a Compliance Plan (the "General Compliance Plan") governing compliance by Provider and its workforce with all laws applicable to Provider's health care business.

The HIPAA Compliance Plan is supplemental to the General Compliance Plan and sets forth certain administrative policies and procedures related to hiring and employment, education and training, monitoring, compliance and reporting of violations. To reduce duplication, Provider intends that the administrative policies set forth in this HIPAA Plan will apply with equal force and effect to the training, education, monitoring and reporting of matters addressed in the General Compliance Plan as applicable. Accordingly, any reference to "laws" in the administrative policies and procedures of this HIPAA Plan shall refer specifically to the laws the subject matter of which are referenced in the General Compliance Plan.

#### **BASIC PRINCIPLES**

The following Standards of Conduct Regarding Privacy and Security summarize the basic principles upon which Provider's HIPAA Compliance Program is based. These Standards apply to all of Provider's directors, officers,

employees, and independent contractors, as well as all employees and agents of American Physician Services, Inc. (the "Manager"), who performs services for Providers (the "Provider Personnel"). These Standards must be carefully reviewed and closely followed by all Provider Personnel. Supplementary information relating to these Standards can be found in the HIPAA Compliance Program Manual and will be provided through periodic formal and informal training and education programs. Any employee who has questions concerning these Standards should seek guidance from Provider's Privacy Officer. Each employee must complete and sign the Certification attached to these Standards of Conduct Regarding Privacy and Security indicating that he or she has read, understands, and will comply with these Standards of Conduct Regarding Privacy and Security.

**Standard No. 1**

**Participation In the Compliance Program**

*Participation in Provider's HIPAA Compliance Program is a condition of employment and is a factor that will be considered in each employee's performance evaluation.*

Compliance may begin with the development of a HIPAA Compliance Program Manual and Standards of Conduct Regarding Privacy and Security, but it does not end there. A HIPAA Compliance Program cannot be effective unless each and every employee actively participates in the Program by carefully reviewing these Standards of Conduct Regarding Privacy and Security and attending Provider training and education programs. Participation in Provider's HIPAA Compliance Program is a condition of employment and will be a factor considered in each employee's performance evaluation. As such, it will affect decisions relating to compensation, promotion and retention.

**Standard No. 2**

**Compliance With Laws, Policies and Procedures**

*Compliance with applicable federal and state laws on health information privacy and HIPAA Compliance Program policies and procedures is a condition of employment at Provider.*

Provider offers services that are heavily regulated and subject to a large number of federal and state civil and criminal laws and regulations. Violation of these laws and regulations can result in financial penalties and in some cases, imprisonment. Provider's HIPAA Compliance Program is designed to prevent such violations. Accordingly, it is critical that all Provider employees comply with the privacy laws and regulations that are applicable to Provider's business and

with all HIPAA Compliance Program policies and procedures. Such compliance is a condition of employment and is a factor that will be considered in each employee's performance evaluation.

**Standard No. 3**  
**Privacy Compliance Questions**

*If a Provider employee has a question concerning whether a particular practice violates applicable health information privacy laws or Provider's HIPAA Compliance Program policies or procedures, that employee should not guess as to the correct answer; he or she should seek guidance from his or her supervisor or the Privacy Officer.*

Health information privacy laws and regulations, such as HIPAA are numerous and complicated. Although one of the objectives of Provider's HIPAA Compliance Program is to educate all Provider employees about the basic requirements of these laws and regulations, Provider does not expect all of its employees to become experts. For precisely this reason, where an employee is not sure whether a particular activity or practice violates the privacy laws (or any of the HIPAA Compliance Program policies and procedures), the employee should not — under any circumstances — “guess” as to the correct answer. Instead, the employee should seek guidance from his or her supervisor or the Privacy Officer. Most simply put, when in doubt about the meaning or requirements of the law or Provider's HIPAA Compliance Program policies or procedures, ask the appropriate Provider personnel. Provider employees will not be penalized for asking privacy or security compliance-related questions. To the contrary, Provider is intent on creating a culture in which every employee is comfortable asking the questions necessary to ensure that he or she understands his or her tasks and obligations in full.

**Standard No. 4**  
**Violations, Confidentiality, Non-Retaliation**

*If a Provider employee believes that an existing practice may violate privacy laws or the HIPAA Compliance Program policies or procedures, the employee must report this practice. This report may be made anonymously. Further, Provider will not take any adverse action against an employee who makes such a report in good faith and who was not involved in the practice at issue.*

Although the primary objective of Provider's HIPAA Compliance Program

is to prevent violations of applicable health information privacy laws, no system or person is perfect. Where such a violation may have occurred, Provider needs to conduct a prompt and thorough investigation of the suspected misconduct. This investigation will allow Provider to determine whether a violation has occurred and, if so, what remedial measures or disciplinary action, if any, to take. Accordingly, all employees are required, as a condition of employment, to report suspected unauthorized uses or disclosures of Protected Health Information or other misconduct. Reports of suspected misconduct may be made to a supervisor, the Privacy Officer or any member of Provider's Privacy Committee in writing or verbally. If a report is made in writing, the report does not need to include the identity of the person making the report.

In all events, Provider will strive to maintain the confidentiality of any reporting employee. However, it must be understood that there may be a time where a reporting employee's identity may become known or may have to be revealed (e.g., if government authorities become involved in the investigation). Finally, whether or not the identity of a reporting employee becomes known or is revealed, under no circumstances will Provider take adverse action against a Provider employee who reports actual or potential misconduct in good faith and who was not involved in the misconduct in question.

**Standard No. 5**  
**Truth, Accuracy and Completeness**

*Provider employees must be truthful in all of their communications with private and governmental organizations.*

All documents prepared by Provider employees, and all data entered into Provider's systems by employees, whether for internal or external use or processing, must be truthful, accurate and complete. All employees shall carefully follow HIPAA Compliance Program policies and procedures relating to protected data access, use, disclosure, and retention.

**Standard No. 6**  
**Patient Confidentiality**

*Provider employees must protect the privacy of medical and other information received from and about patients and potential patients.*

As part of Provider's business, it receives medical and other personally identifiable health information from various health care providers and payors, including information relating to such individual patients' medical conditions. Provider will respect and preserve the privacy of this personal information. Except to the extent permitted by the patient and under state and federal law,

Provider and its employees will not disclose personally identifiable health information about a patient to any third party. Furthermore, Provider is required to preserve the confidentiality of patient information that remains in its possession.

### **Disciplinary Action**

Provider will take disciplinary action, ranging from a verbal warning to termination of employment, against any employee, regardless of his or her level or position, who fails to comply with these Standards of Conduct Regarding Privacy and Security, HIPAA Compliance Program policies and procedures, or applicable health information privacy laws. The severity of the disciplinary action, which will be determined by senior management (in consultation with the Privacy Officer and the employee's supervisor, as appropriate), will generally depend on a variety of factors, including but not limited to: (1) the severity of the violation, (2) whether the violation was committed intentionally, recklessly, negligently, or accidentally, (3) whether the employee has committed any violations in the past, (4) whether the employee self-reported his or her misconduct, and (5) whether (and the extent to which) the employee cooperated with Provider in connection with its investigation of the misconduct. Certain actions that fail to comply with these Standards of Conduct Regarding Privacy and Security, HIPAA Compliance Program policies and procedures, or applicable health information privacy laws, may be subject to discipline, up to and including termination, without regard to these factors or some of them, because of the seriousness of the issues involved. Where this is the case, the disciplinary policy and factors involved will be described in a policy or procedure. Where appropriate, Provider may also take disciplinary action against supervisors who fail to detect or report misconduct on the part of employees under their supervision.

### **Remedial Action**

In addition to taking disciplinary action, Provider will implement other remedial measures, as appropriate, in the event of a violation of these HIPAA Compliance Program Standards of Conduct Regarding Privacy and Security, policies and procedures or applicable health information privacy laws. The remedial action may include, for example, education of employees, modification of systems, and modifications of policies and procedures, to prevent violations of these laws.

### **Certification**

As part of the implementation of the HIPAA Compliance Program, each Provider employee must certify and agree in writing that he or she has read, understands and will comply with these Standards of Conduct Regarding Privacy and Security. The certification will be renewed by each employee on an annual

basis. In addition, a new employee must execute the certification and agreement prior to commencing work for Provider.

*Standards of Conduct Regarding Privacy and Security*  
*Originally Adopted- April 14, 2003*  
*Revised: \_\_\_\_\_*