

Re: **The HIPAA Privacy Rule – Practical Steps Toward Compliance**

Dear Client:

If you are like most health care providers, you are probably wondering where you fit into the labyrinth of HIPAA compliance. You are likely being bombarded by literature and advertisements for various compliance products and programs. Many of these goods and services are costly and may seem comparable to hitting a nail with a sledgehammer. Nevertheless, the April 14, 2003 deadline is approaching and you cannot postpone your compliance efforts. You should know that it is relatively simple and affordable to meet the Privacy Rule's basic requirements. We will endeavor in this brief article to provide you with a summary of the services that our firm can provide to assist you.

### **BASIC DESCRIPTION OF THE PRIVACY RULE**

The Privacy Rule establishes a national "floor" of privacy standards to protect "individually identifiable health information," which is defined as a subset of health information, including demographic information that is: *created by or received by a covered entity; **and** related to the past, present or future physical or mental health condition of an individual, provision of care to an individual or payment for such care; **and** **which** identifies the individual; **or** may provide a reasonable basis to believe that the information can be used to identify the individual.* The Privacy Rule protects all medical records and individually identifiable health information (hereinafter, Protected Health Information or "PHI") held or disclosed by a covered entity in any form, whether communicated electronically, on paper or orally. The Privacy Rule also requires covered entities to maintain appropriate administrative, technical and physical safeguards to ensure the integrity of PHI; to protect against reasonably anticipated threats to the security of PHI; and to ensure compliance with the Privacy Rule by the entity's employees.

### **IS MY PRACTICE A COVERED ENTITY?**

The first essential step is determining whether your entity is covered by the Privacy Rule. The Privacy Rule covers health plans, health care clearinghouses and health care providers who conduct certain financial and administrative transactions (i.e., billing; transfers of funds) electronically.

### **WHAT ARE "REASONABLY ANTICIPATED THREATS?"**

It is impossible to predict the myriad possible threats to the security of PHI, and it is difficult to speculate upon the circumstances that will result in a certain violation of the Privacy Rule. However, the Privacy Rule is clear in its mandate that entities maintain a high level of security to protect against all reasonably anticipated threats to the integrity of PHI. This mandate requires planning with an eye toward prevention. Consider scenarios that could give rise to prosecution of your practice for failing to maintain adequate safeguards, such as wrongful conduct by a disgruntled employee. It is important to protect against such a scenario.

### **THE IMPORTANCE OF GAP ANALYSIS**

You may already have measures in place to protect the security and privacy of medical records, and mistakenly believe that the Privacy Rule only applies to entities that lack such protections. Regardless of your current habits, gap analysis is the essential next step. Gap analysis is the process by

which you examine the basic requirements of the law against the backdrop of your practice’s needs, routines and procedures. Your current activities may fall within a continuum of compliance; that is, some activities are “almost” compliant and require only minor tweaking, while other activities run completely afoul of the law and will result in a violation of the law if major changes aren’t implemented before the compliance deadline. Frier & Levitt (“F&L”) can assist you in performing a gap analysis of your practice’s habits and the requirements of the Privacy Rule.

### **TAILORING A COMPLIANCE PROGRAM TO YOUR PRACTICE**

Because each practice presents its own unique needs and challenges, there is no “one-size-fits-all” approach to compliance. You must examine the day-to-day functioning of your practice to ensure that your efforts abide the requirements of the Privacy Rule in both form and substance. Because you are in the best position to understand your practice’s internal functioning and special needs, your insight is the most important ingredient in a successful compliance program. The following questions, though not exhaustive, should help you to begin your own preliminary gap analysis.

<b>Regulatory Requirement</b>	<b>Gap Analysis Question to Consider</b>
Individuals will be entitled to a clear written explanation of how an entity uses, keeps and discloses the individual’s PHI	Does your practice provide to patients a clear written policy, which describes in lay terms, the manner in which it uses, keeps and discloses PHI? F&L will provide you with a HIPAA Privacy Manual, along with the proper notices to patients.
Covered entities must know the circumstances under which a patient authorization should be obtained and must track disclosures for non-routine purposes (i.e., other than treatment or payment purposes)	Does the practice have an established policy for obtaining a patient’s authorization for non-routine uses or disclosures of PHI? F&L will provide you with appropriately drafted authorizations and simple, efficient systems for recording non-routine disclosures.
Individuals will be able to inspect and receive copies of their records and request amendments thereto, although an entity need not abide a request to change a record that is complete and accurate	F&L will include in your Manual policies regarding patients’ inspections of their records (and reasonable requests for amendments thereto) that honor the patient’s rights while avoiding undue disruption to your practice.
Except where a patient has authorized the disclosure, covered entities must employ reasonable safeguards to ensure that only the “minimum necessary” information is disclosed.	F&L will instruct your staff to take reasonable safeguards to protect patients’ privacy, such as discussing/disclosing only the relevant aspects of a patient’s history, care and treatment.

<p>Family members may not be given information regarding an individual's PHI unless the individual expressly consents to such disclosure.</p>	<p>If physicians or other staff members interact with patient's families, they must obtain the patient's express permission to disclose the patient's PHI to a family member. Even with a patient's consent, only the minimum necessary information may be shared. F&amp;L will train your staff to deal politely, but firmly, with the inquiries of a patient's family members.</p>
<p>Agreements with other entities must contain the required terms for business associate contracts under the Privacy Rule.</p>	<p>F&amp;L will review, and if necessary, renegotiate your business associate contracts.</p>

### **PENALTIES FOR FAILURE TO COMPLY WITH THE PRIVACY RULE**

The Privacy Rule will be enforced by the Department of Health and Human Services' Office for Civil Rights and violations could result in significant criminal liability, as well as potential civil litigations exposure. Furthermore, federal criminal liability will apply if a covered entity knowingly and improperly discloses information or obtains information under false pretenses. Violation-specific penalties include: up to \$50,000 and one year in prison for obtaining or disclosing protected health information; up to \$100,000 and up to five years in prison for obtaining protected health information under false pretenses; and up to \$250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

### **CONCLUSION**

We hope that this brief summary of the HIPAA Privacy Rule has helped you to assess your practice's compliance needs. If you are interested in Frier & Levitt's compliance services, please contact our office.