

January 2005

RE: HIPAA Security Rule

Dear Client:

Now that we have all adjusted to the requirements of the Privacy Rule under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), another compliance deadline is fast approaching. By April 20, 2005, all covered entities that electronically store or transmit protected health information ("ePHI") must develop and implement a program to comply with the Security Rule. This letter explains some of the requirements of the Security Rule and how Frier and Levitt, LLC may assist you in your compliance efforts.

I. How does the Security Rule differ from the Privacy Rule?

The main difference between the Security Rule and the Privacy Rule is that while the Privacy Rule covers all protected health information whether it is on paper or transmitted orally, the Security Rule specifically seeks to protect ePHI that is stored or transmitted electronically. Therefore, the scope of the Security Rule and its related requirements is focused on the integrity of electronic protected health information (e.g. ePHI). So, covered entities that collect, maintain, use or transmit protected health information in electronic form must implement reasonable and appropriate administrative, physical and technical safeguards to ensure the integrity, availability and confidentiality of ePHI.

II. What does the Security Rule require from Covered Entities?

Like the Privacy Rule, the Security Rule requires the development and implementation of policies and procedures geared towards protecting ePHI and also requires that members of your workforce be trained on how such procedures should be implemented. Similarly, the Security Rule requires covered entities to enter into business associate agreements with third parties who have access to your ePHI or amend existing business associate agreements to address the requirements of the Security Rule.

There are three main areas of focus in the Security Rule: 1) Administrative Safeguards; 2) Physical Safeguards and 3) Technical Safeguards. When implementing such safeguards, it is important to note that the Security Rule is intended to be scalable and technology neutral. Therefore, the Security Rule will not mandate the use of a certain technology for compliance. It is flexible so that a covered entity may use reasonable and appropriate measures to comply with the Security Rule depending on the size and complexity of the covered entity, the amount of ePHI stored or transmitted by the covered entity, the cost of compliance and the degree of risk associated with the ePHI.

In the implementation of the Administrative, Physical and Technical Safeguards, it is important to note that certain safeguards are "addressable" and certain safeguards are "required." Obviously, a covered entity must comply with the "required" safeguards. Addressable safeguards are designed to make the Security Rule flexible and scalable based upon the specific characteristics of a covered entity. While certain safeguards are "addressable" they are not intended to be optional; rather, a covered entity may use reasonable and appropriate measures to

comply with the addressable safeguards. It is important to note that the Department of Health and Human Services specifically stated in its response to comments on the Security Rule that “[c]ost is not meant to free covered entities from this responsibility.”

III. Integration with the Privacy Rule

Because certain requirements of the Security Rule will expand on existing Privacy Rule policies and procedures, there may be areas where the integration of both compliance programs is appropriate. For example, business associate agreements are also required under the Security Rule to ensure that your third party vendors are obligated to maintain the confidentiality, integrity and availability of ePHI. Your practice may have an existing business associate agreement with a third party vendor who has access to or performs a service using your ePHI. This business associate agreement must be revised to reflect the requirements of the Security Rule. There may also be policies and procedures in your Privacy Rule manual that deal with physical safeguards for maintaining the integrity of ePHI (e.g. a policy and procedure to require that computers be password protected). When overlap occurs, the policy and procedure manuals for both rules should be integrated so that they are consistent and applied in a uniform manner.

IV. Frier and Levitt Services

As with the Privacy Rule, Frier & Levitt can develop a Security Rule Compliance Program for your office. Our services will include the following:

- 1) Risk Analysis. We will conduct a “risk analysis” to determine the potential risk and vulnerabilities to the confidentiality, integrity and availability of your ePHI;
- 2) Policy and Procedure Manual. Based upon the risk analysis, we will prepare a formal written policy and procedure manual for your practice. We will review your existing Privacy Rule policy and procedure manual to determine when integration of both manuals is necessary;
- 3) Business Associate Agreements. We will analysis your practice to determine your business associates and prepare the necessary business associate agreements. When appropriate, we will revise existing business associate agreements so that they also comply with the Security Rule;
- 4) Training. Once the risk analysis and policy and procedure manual are complete, we will perform a training session for members of your workforce.

Estimated fees for a Security Rule Compliance Program are based upon the total number of employees, including physicians, of your practice. Actual fees may vary depending on your practice’s unique needs and circumstances. Frier & Levitt will advise you in advance if the actual costs are expected to exceed the estimated costs provided below.

If you have any questions about this letter or are interested in utilizing our services, please do not hesitate to contact us.