

## Health Plans and Employers Who Sponsor Them Face Additional HIPAA Requirements

*New Security Measures Required by April 21, 2005*

**September 29, 2004**

By now, you are probably familiar with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the many requirements it imposes on group health plans (and the employers that sponsor them), health care providers, and health care clearinghouses (collectively known as covered entities). You may not know, however, that as of April 20, 2005, covered entities will also be required to comply with the HIPAA Security Rule.

The Security Rule imposes additional requirements, designed to define the “administrative, physical and technical safeguards” necessary to “ensure the confidentiality, integrity and availability of all electronic protected health information (ePHI),” and to “protect against any reasonably anticipated threats or hazards to the security or integrity of [the ePHI] and protect against any reasonably anticipated” improper uses or disclosures of the ePHI. More specifically, the rule requires covered entities to establish security policies and procedures, including training programs, that limit access to and ensure the confidentiality and integrity of any ePHI that they create, receive, maintain or transmit. It is important to note that, unlike the Privacy Rule, the Security Rule applies to electronic information only, such as Internet transmissions and computerized information, and not to paper files. However, the Privacy Rule continues to apply to hard copy and paper PHI, as well as ePHI.

### **How the Rule Will Impact Your Business**

As a general matter, if your company’s health plan is a covered entity, the rule will require that you implement reasonable and appropriate measures to ensure the security of ePHI in computers, workstations, servers and networks, and that you make sure that access is limited to authorized users. More precisely, the Security Rule sets out defined standards, which must be met, with implementation specifications that are either required or addressable. If a specification is required, you must implement it.

If a specification is addressable, however, the rule requires you to assess whether it is a reasonable and appropriate safeguard to apply to your company’s particular security

systems. Whether a specification is reasonable and appropriate will depend on a variety of factors unique to your company, such as: the results of your risk analysis, your risk mitigation strategy, your current security measures and the cost of implementation. If you conclude that it is reasonable and appropriate, you must implement the safeguard. On the other hand, if you find that implementing the safeguard is neither reasonable nor appropriate, the rule requires that you: (1) document why it would not be reasonable and appropriate; and (2) either implement an equivalent or alternative measure that is reasonable and appropriate and document the reasons for the use of an alternative to meet the standard, or take no action with regard to the specification, and document why no action was taken and how the standard is being met.

Thankfully, as with the Privacy Rule, the Security Rule standards are scalable, so that when implementing the rule, the size, complexity, capabilities and technical infrastructure of the entity-as well as the costs and potential risks of security measures-are taken into account.

### **How Morgan Lewis Can Help**

Morgan Lewis lawyers recommend that you appoint a security official and begin an internal risk analysis as soon as possible to ensure compliance by the deadline. We have helped numerous companies and their health plans successfully meet the compliance obligations of the Privacy Rule, and are now assisting businesses with Security Rule compliance.

As you start to think about your obligations under the Security Rule, we recommend that you consider the following steps:

1. Appoint a security official.
2. Conduct a risk analysis audit, and analyze the results of the audit to determine where ePHI is collected and maintained at your company, the status of your electronic systems, and the amount of work that needs to be done to comply with the Security Rule. The Privacy Officer, Security Official, and HR, IT and Legal Department personnel should be involved in this analysis.
3. Implement and/or address the Implementation Specifications.
4. Develop, implement and document the policies and procedures related to the Security Rule.
5. Amend the plan document to include Security Rule provisions, and ensure that the business associate agreements include Security Rule provisions.

We can help you meet these compliance goals. Our attorneys, working in combination with technology consultants and vendors, can help you conduct the risk analysis audit and determine which security measures to adopt, and can help you assess your liabilities and obligations in light of your audit results, risk mitigation strategy, size and complexity,

current security measures, and technical infrastructure. We can also help to assess the potential risk to ePHI and the cost of implementing security measures. We can also assist in preparing the required documentation. Furthermore, we would be more than happy to put you in contact with technology consultants and vendors that will be able to assist you in conducting a risk analysis and implementing a thorough compliance program.

### **Contact Us**

If you have any questions about the information in this document, or would like to further discuss compliance with the Security Rule, please contact:

#### **Dallas**

Riva T. Johnson	215.438.1557	riva.johnson@morganlewis.com
-----------------	--------------	------------------------------

#### **Philadelphia**

Steven D. Spencer	215.963.5714	sspencer@morganlewis.com
Robert L. Abramowitz	215.963.4811	rabramowitz@morganlewis.com
Georgina L. O'Hara	215.963.5188	gohara@morganlewis.com
Mims Maynard Zabriskie	215.963.5036	mzabriskie@morganlewis.com

#### **San Francisco**

Mark H. Boxer	415.442.1695	mboxer@morganlewis.com
---------------	--------------	------------------------

#### **Washington, D.C.**

Margery Sinder Friedman	202.739.5120	mfriedman@morganlewis.com
Jessica Bernanke	202.739.5447	jbernanke@morganlewis.com

### **About Morgan, Lewis & Bockius LLP**

With 1,200 lawyers in 19 offices worldwide, Morgan Lewis offers seamless service across practice areas and offices. A fully integrated, multipractice global law firm, Morgan Lewis assists clients with all of their legal needs, from day-to-day business decisions to the most complex global deals and litigation.