

## HIPAA PRIVACY AND SECURITY UPDATE

April 30, 2003

The HIPAA Privacy Rule became effective on April 14, 2003. All health plans, health care clearinghouses, and health care providers who transmit electronic health care information are required to be in compliance with significant privacy rule requirements. The rule allows patients to file complaints to the Department of Health and Human Services ("HHS"), which can then pursue civil and/or criminal penalties, including a \$250,000 fine and 10 years in prison for the most serious offenses. Health care organizations that have thus far neglected their compliance efforts may now have a limited amount of time to avoid the risk of enforcement proceedings.

### **HIPAA Privacy Enforcement Regulations Released**

HHS has published an interim final rule, with a request for comments, establishing rules of procedure for imposing civil monetary penalties on covered entities that violate HIPAA privacy, security or electronic transaction standards. While the rule acknowledges that HHS intends to seek to promote "voluntary compliance" by covered entities and that HIPAA enforcement would be a complaint driven process, the interim rules of procedure are intended to inform covered entities of the agency's approach to enforcement and advise them of certain procedures that will be followed. "The duty to comply with certain of the HIPAA rules is now a reality for many, if not most, covered entities. The immediacy of the compliance obligation brings with it the issue of how these rules will be enforced," the preamble states. The provisions contained in the rule describe procedures related to issuing subpoenas, the notice of proposed civil monetary penalty determination, authorities to settle, requesting a hearing before an Administrative Law Judge, pre-hearing conferences, settlement, discovery, and fees. The rules do not specify what activities will constitute violations of HIPAA or how specific penalty amounts will be calculated, leaving those substantive issues for future rulemaking.

### **Final HIPAA Security Regulations Published**

HHS recently published the security regulations applicable under HIPAA. The HIPAA Security Standards require health plans, health care clearinghouses, and health care providers that electronically maintain or transmit individually identifiable health information to implement reasonable and appropriate administrative, technical, and physical safeguards to ensure the integrity and confidentiality of such information. Additionally, business associates of a covered entity must contract with the covered entity to implement safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that they create, receive, maintain, or transmit on behalf of the covered entity. Business associates must also ensure that any agent or subcontractor to whom they provide electronic protected health information agrees to implement similar safeguards to protect that information.

The HIPAA Security Standards allow a covered entity to choose security measures that are reasonable and appropriate for that entity. In selecting which security measures to adopt, a covered entity should consider its size, its complexity, its electronic capabilities, the costs of the security measures, and the potential risks to its electronic protected health information. The HIPAA standards have two categories: "required" and

"addressable." All covered entities must implement "required" standards. A covered entity does not need to implement "addressable" standards if they are not reasonable or appropriate for an organization of the size and nature of the covered entity, however the covered entity may have to implement an alternative. A chart summarizing the Security Standards is provided below. A comprehensive analysis of the HIPAA Security Rule is available on our website at [www.millerholguin.com/library/whats\\_new.cfm](http://www.millerholguin.com/library/whats_new.cfm)

<b>SECURITY STANDARDS</b>	
<b>ADMINISTRATIVE SAFEGUARDS</b>	<b>PHYSICAL SAFEGUARDS</b>
STANDARD	STANDARD
<b>Security Management Process</b> <ul style="list-style-type: none"> <li>• Risk Analysis (R)</li> <li>• Risk Management (R)</li> <li>• Sanction Policy (R)</li> <li>• Information System Activity Review (R)</li> </ul>	<b>Facility Access Controls</b> <ul style="list-style-type: none"> <li>• Contingency Operations (A)</li> <li>• Facility Security Plan (A)</li> <li>• Access Control &amp; Validation Procedures (A)</li> <li>• Maintenance Records (A)</li> </ul>
<b>Assigned Security Responsibility</b> (R)	<b>Workstation Use</b> (R)
<b>Workforce Security</b> <ul style="list-style-type: none"> <li>• Authorization/Supervision (A)</li> <li>• Workforce Clearance Procedure (A)</li> <li>• Termination Procedures (A)</li> </ul>	<b>Workstation Security</b> (R)
<b>Information Access Mgmt.</b> <ul style="list-style-type: none"> <li>• Isolating Health Care Clearinghouse Functions (R)</li> <li>• Access Authorization (A)</li> <li>• Access Establishment &amp; Modification (A)</li> </ul>	<b>Device &amp; Media Controls</b> <ul style="list-style-type: none"> <li>• Disposal (R)</li> <li>• Media Re-use (R)</li> <li>• Accountability (A)</li> <li>• Data Backup &amp; Storage (A)</li> </ul>
<b>Security Awareness &amp; Training</b> <ul style="list-style-type: none"> <li>• Security Reminders (A)</li> <li>• Protection from Malicious Software (A)</li> <li>• Log-in Monitoring (A)</li> <li>• Password Management (A)</li> </ul>	<b>TECHNICAL SAFEGUARDS</b>
<b>Security Incident Procedures</b> <ul style="list-style-type: none"> <li>• Response &amp; Reporting (R)</li> </ul>	STANDARD
<b>Contingency Plan</b> <ul style="list-style-type: none"> <li>• Data Backup Plan (R)</li> <li>• Disaster Recovery Plan (R)</li> <li>• Emergency Mode Operation Plan (R)</li> <li>• Testing &amp; Revision Procedures (A)</li> <li>• Applications &amp; Data Criticality Analysis (A)</li> </ul>	<b>Access Control</b> <ul style="list-style-type: none"> <li>• Unique User ID (R)</li> <li>• Emergency Access Procedure (R)</li> <li>• Automatic Logoff (A)</li> <li>• Encryption &amp; Decryption (A)</li> </ul>
<b>Evaluation</b> (R)	<b>Audit Controls</b> (R)
<b>Business Associate Contracts &amp; Other Arrangements</b> <ul style="list-style-type: none"> <li>• Written Contract or Other Arrangement (R)</li> </ul>	<b>Integrity</b> <ul style="list-style-type: none"> <li>• Mechanisms to Authenticate EPHI (A)</li> </ul>
	<b>Personal or Entity Authentication</b> (R)
	<b>Transmission Security</b> <ul style="list-style-type: none"> <li>• Integrity Control (A)</li> <li>• Encryption (A)</li> </ul>
	<u>Notes</u>
	(A) Standard is addressable. Health care organizations do not need to implement the standard if it is not reasonable or appropriate, but the organization may have to implement an alternative.
	(R) Standard is required.

If you have any questions regarding HIPAA Privacy or Security, please call Michael A. Dowell, J. Robert Liset, Dale S. Miller, Henry A. Holguin, Judy D. Vaccaro, or Robert A. Polisky.

Copyright © 2003 Miller & Holguin