Honigman Miller Schwartz and Cohn's *February 2003*

HIPAA LAW FOCUS

A Special Joint Newsletter on the HIPAA Privacy Rule
Prepared by the
Health Care and Employee Benefits Departments of HMS&C

DHHS ISSUES FINAL SECURITY STANDARDS

On February 20, 2003, the Secretary (Secretary) of the United States Department of Health and Human Services (DHHS) published the final security standards (the Security Rule) implementing the security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Security Rule mandates national standards for the integrity, confidentiality and availability of electronic protected health information. Compliance with the Security Rule generally is required by April 20, 2005 or April 20, 2006 for small health plans (*i.e.*, those with annual receipts of $5 million or less). The Preamble to the Security Rule, however, indicates that the compliance date is April 21, 2005, and April 21, 2006 for small health plans.

Although the Security Rule applies to covered entities as defined by the Standards for Privacy of Individually Identifiable Health Information issue d under HIPAA (the Privacy Rule), the scope of the Security Rule is more limited than the Privacy Rule. The Security Rule only applies to PHI transmitted or maintained in electronic form and contains no standards for protecting health information in non-electronic forms. Importantly, however, the Security Rule does not distinguish between either: (1) the movement of data within the covered entity and the movement of data between the covered entity and others, or (2) data in transmission and data at rest (*i.e.*, in storage or memory). All such data is subject to the Security Rule.

CHANGES FROM THE PROPOSED SECURITY RULE

The Security Rule builds upon the proposed rule published on August 12, 1998, though with some important differences.

First, the Security Rule is more "technology-neutral" than the proposed rule. This neutrality reflects both DHHS' concern that the security requirements be "scalable" to covered entities of varying sizes, budgets and organizational sophistication and its recognition of the impact of the rapid pace of technological change.

Second, the Security Rule places greater emphasis on flexibility, which gives covered entities more leeway in determining how to comply. "Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement standards and implementation specifications as specified in this subpart." The downside to this flexibility, of course, is that a covered entity may not always be certain that it has met the Security Rule requirements. DHHS has pledged to issue further guidance.

Third, the Security Rule no longer requires chain of trust agreements. They have been replaced by a requirement that business associate contracts required by the Privacy Rule contain certain provisions that obligate the business associate to secure electronic PHI that it creates or maintains on behalf of the covered entity in the same manner as the covered entity.

Finally, the regulation of electronic signatures has been eliminated from the Security Rule. DHHS intends to issue a separate rule with respect to electronic signatures.

GENERAL STRUCTURE OF THE SECURITY RULE

The Security Rule is structured as: (1) a set of general requirements, (2) a series of articulated standards, and (3) a series of implementation specifications designed to meet the standards.

The General Requirements.

The general standard set forth under the Security Rule requires that covered entities:

- Ensure the confidentiality, integrity and availability of all electronic PHI that it creates, receives, maintains or transmits.
- Protect against any reasonably anticipated hazards.
- Protect against any reasonably anticipated uses or disclosures that are neither permitted nor required under the Privacy Rule.
- Ensure compliance with the Security Rule by its workforce.

The Articulated Standards.

To meet these general requirements, each covered entity must meet clearly articulated standards in the areas of administrative, physical and technical safeguards. There are 22 standards in the Security Rule (four of which are not listed in Appendix A of the Security Rule).

HMSC Observation. *The Privacy Rule requires covered entities to implement "appropriate administrative, technical and physical safeguards" to protect PHI in all forms. This requirement generally takes effect April 14, 2003. Thus, while compliance with the Security Rule generally is not required until much later, the processes outlined in the Security Rule will be useful to guide covered entities in determining how best to comply with the security provisions of the Privacy Rule.*

The Implementation Specifications.

The implementation specifications set forth what covered entities actually must do to meet the standards. Importantly, the implementation specifications come in two varieties: "**required**" and "**addressable**." **Required** implementation specifications are, as the name implies, an action or undertaking that a covered entity must take to comply with the articulated standard.

Addressable specifications represent steps that covered entities must consider, but need not implement. The covered entity must make a reasonable determination whether, given its circumstances, the specification set forth in the Security Rule should be implemented, or whether an equivalent alternative measure should be implemented. The factors that a covered entity may consider in making this determination are:

- its size, complexity and organizational capabilities,
- its technical infrastructure,
- the costs involved, and
- the probability and criticality of the risks to PHI that are involved.

It is conceivable that a covered entity could reasonably determine that no implementation step is required. Once it reaches a conclusion about the specification, the covered entity must document in writing (including electronic formats) its decision not to implement the **addressable** implementation specification, the rationale for that decision and the alternative safeguard it chose to implement.

The requirements set forth in the standards and implementation specifications are considered to be a "floor" for securing electronic PHI. Covered entities and their business associates, of course, are free to implement stricter, more stringent protective measures for any of the standards.

HMSC Observation. *Note that the Security Rule does not include implementation specifications for every standard and, in some cases, there are only* ***required*** *or* ***addressable*** *implementation specifica-tions. These implementation specifica-tions offer welcome flexibility for Security Rule compliance by covered entities, but also create some uncertainty about whether any particular security effort is adequate.*

ADMINISTRATIVE STANDARDS AND IMPLEMENTATION SPECIFICATIONS

Security Management Process Standard.

A covered entity must implement policies and procedures to prevent, detect, contain and correct security violations to eliminate or minimize potential risks or vulnerabilities. DHHS notes that covered entities have flexibility to implement this standard based on numerous factors, such as size, degree of risk and environment.

The **required** implementation specifications for this standard require a covered entity to:

- Conduct an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI.
- Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level as required by the Security Rule.
- Apply appropriate sanctions against workforce members who fail to comply with the covered entity's security policies and procedures.
- Implement procedures regularly to review records of information system activity (such as audit logs, access reports and security incident tracking reports).

HMSC Observation. *This standard sets the baseline for a covered entity's entire compliance program under the Security Rule. It requires every covered entity to undertake a risk assessment and risk analysis that should guide the covered entity's compliance efforts. In determining what security measures are reasonable and appropriate to implement, the covered entity will have to continuously return to those baseline risk assessments in adopting appropriate levels of security are required and what steps need to be taken to reach those levels.*

Assigned Security Responsibility Standard.

A covered entity must identify a security official responsible for the development and implementation of the covered entity's security policies and procedures. The security official's responsibilities would include: (1) the use of security measures to protect electronic PHI, and (2) the conduct of personnel in relation to the protection of electronic PHI. The Security Rule requires the designation of a single security official to ensure accountability within each covered entity. In larger organizations, more than one individual may be given specific security responsibilities, but a single individual must have final responsibility for the security of electronic PHI.

Workforce Security Standard.

A covered entity must implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic PHI and to ensure that workforce members without authorization and/or supervision do not have such access. To implement the workforce security standard, the **addressable** implementation specifications are to:

- Provide for proper authorization and/or supervision of workforce members who work with electronic PHI or in a location in which electronic PHI may be accessed.

- Determine that the access of workforce members to electronic PHI is appropriate.

- Terminate access to electronic PHI when a workforce member is terminated or when access to electronic PHI by such member is determined to be inappropriate (*e.g.*, changing combination locks, removing the member from access lists, eliminating the user's account or requiring relinquishment of keys, tokens or cards that allow access).

DHHS explains that these implementation specifications are **addressable** because, in certain circumstances, formal procedures may not be necessary, such as for a solo physician whose entire staff consists of the physician and his or her spouse.

HMSC Observation. *Instead of the proposed rule's requirement to obtain background checks on workforce members, the Security Rule now includes an optional screening process; the need and extent for such process is based upon a covered entity's assessment of risk, cost, benefit and feasibility, as well as on the protective measures already in place.*

Information Access Management Standard.

A covered entity must implement policies and procedures for authorizing access to electronic PHI. These policies and procedures must define the levels of access for all personnel authorized to access electronic PHI and how access is granted or modified.

The **required** implementation specifications for this standard provide that if a health care clearinghouse is part of a larger organization (that is not a covered entity), the larger organization must assure that the health care clearinghouse function has instituted measures to ensure that electronic PHI that it processes is not improperly accessed by unauthorized persons or other entities, including the larger organization. Internal electronic communication within the larger organization will not be covered by the Security Rule if it does not involve the health care clearinghouse.

The **addressable** implementation specifications call for implementing policies and procedures:

- For granting access to electronic PHI.

- That establish, document, review and modify a user's right of access to a workstation, transaction, program or process.

Security Awareness and Training Standard.

A covered entity must implement a security awareness and training program for all workforce members, including management. Covered entities only are required to provide training to workforce members who have access to electronic PHI. Business associates, however, must be made aware of security policies and procedures, whether through contract language or other means.

The **addressable** implementation specifications with respect to security awareness and training are:

- Periodic security updates.

- Procedures for guarding against, detecting and reporting malicious software.

- Procedures for monitoring log-in attempts and reporting discrepancies.

- Procedures for creating, changing and safeguarding passwords.

HMSC Observation. *DHHS intends that the Security Rule training will be integrated with the covered entity's overall training program, such as the training required by the Privacy Rule and other laws. The amount and type of training is to be determined by the covered entity and depends on the covered entity's configuration and security risks. For example, pamphlets or copies of*

security policies may be sufficient training for an individual who only will have access to electronic PHI on a short-term basis.

Security Incident Procedures Standard.

A covered entity must implement policies and procedures to address security incidents. The covered entity's information environment will determine what specific action constitutes a security incident, the specific processes for documenting a security incident, what should be included in such documentation and the appropriate response.

The covered entity also must identify and respond to suspected or known security incidents and mitigate the harmful effects of known security incidents to the extent practicable. All security incidents and their outcomes must be documented.

HMSC Observation. *Covered entities can take comfort that the Security Rule does not require any security incident reporting to entities outside of the covered entity. Of course, it may be necessary to report such security incidents in order to comply with applicable business policies or other applicable laws.*

Contingency Plan Standard.

Covered entities must establish (and implement, as needed) policies and procedures for responding to an emergency or to occurrences that damage systems housing electronic PHI. Such contingency plans are viewed as the only way to protect the availability, integrity and security of data during unexpected negative events, such as the events of 9/11/01, fires, vandalism, system failures and natural disasters. DHHS notes that contingency plans may be complex or simple depending on the nature and configuration of the entity designing it.

The **required** implementation specifications for this standard include having:

- A data back-up plan, consisting of procedures to create and maintain the ability to retrieve exact copies of electronic PHI.

- A disaster recovery plan, which consists of establishing (and implementing, as needed) procedures to restore any loss of data.

- An emergency mode operation plan, which consists of establishing (and implementing, as needed) procedures to enable the continuation of critical business processes for protecting the security of electronic PHI while operating in emergency mode.

The **addressable** implementation specifications for this standard include:

- Implementing procedures for periodic testing and revision of contingency plans.

- Having applications and data criticality analysis, which consist of assessing the relative critically of specific applications and data in support of other contingency plan components.

Evaluation Standard.

Under this standard, covered entities must perform technical and non-technical evaluations periodically to establish the extent to which their security policies and procedures comply with the Security Rule.

HMSC Observation. *No implementation specifications are indicated for this standard. The Preamble clarifies that evaluations can be performed by an external entity or by a covered entity's own workforce. DHHS will not create certification criteria but encourages professional associations to do so. Additionally, DHHS will not certify any security software or off-the-shelf products, but supports the work of the National Institute of Standards and Technology (NIST), which is working towards that end. Covered*

entities are encouraged to monitor the activities of NIST, which are described at http://nii.nist.gov.

Business Associate Contracts and Other Arrangements Standard.

The concept of chain of trust agreements set forth in the proposed rule has been abandoned. Instead, under the Security Rule, a covered entity can allow a business associate to create, receive, maintain or transmit electronic PHI on its behalf as long as the covered entity receives satisfactory assurances that the business associate will properly safeguard the information. If a covered entity violates the satisfactory assurances it gives as a business associate of another covered entity, it will be in violation of the Security Rule.

1. Exceptions. This standard does not apply to transmissions of electronic PHI:

- By a covered entity regarding the treatment of an individual to a health care provider.
- By a group health plan, HMO or health insurance issuer on behalf of a group health plan to a plan sponsor.
- From or to other agencies providing assistance with health plan eligibility or enrollment determinations or with the collection of PHI when the covered entity is a health plan that is a government program providing public benefits.

2. Documentation. The **required** implementation specifications for this standard require documentation of specific, required satisfactory assurances in a written contract or other arrangement with the business associate. As in the Privacy Rule, if the covered entity is aware of a pattern of activity or practice by a business associate that is a material breach or violation of the business associate's obligation under the contract or other arrangement, the covered entity is in violation of the Security Rule unless it takes reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, the covered entity must terminate the contract (if feasible) or reports the problem to the Secretary of DHHS (if termination is not feasible).

The contract between the business associate and the covered entity must provide that the business associate will:

- Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic PHI that the business associate creates, receives, maintains or transmits on behalf of the covered entity.
- Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it.
- Report to the covered entity any security incident of which it becomes aware.
- Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

DHHS has indicated that it will consider developing sample contract language as it develops guidelines on the Security Rules.

HMSC Observation. *Although compliance with the Security Rule is not required for some time, some covered entities are incorporating these provisions now into business associate contracts required by the Privacy Rule.*

3. Other Arrangements. As in the Privacy Rule, there are circumstances when these business associate agreement requirements are more relaxed. For example, when a covered entity and its business associate are both governmental entities, it is sufficient for the covered entity to enter into a memorandum of understanding with

the business associate that provides the required satisfactory assurances, or if other law contains requirements applicable to the business associate that accomplish those objectives.

Additionally, if a business associate is required by law to perform a function or activity on behalf of a covered entity, or to provide a service to a covered entity that is encompassed by the definition of a business associate, the covered entity can allow the business associate to create, receive, maintain or transmit electronic PHI on behalf of the covered entity as necessary to comply with that law without meeting the implementation specifications noted above, so long as the covered entity tries in good faith to obtain the necessary satisfactory assurances and documents its attempts and why such assurance cannot be obtained. Finally, the covered entity need not obtain authorization to terminate such other contract or arrangement if doing so is inconsistent with the statutory obligations of the covered entity or its business associate.

Group Health Plan Standard.

A group health plan generally must ensure that its plan documents require the plan sponsor to reasonably and appropriately safeguard electronic PHI created, received, maintained or transmitted to or by the plan sponsor on behalf of the group health plan. Exceptions are permitted when the only electronic PHI disclosed to a plan sponsor is for purposes permitted under the Privacy Rule (*i.e.*, PHI consisting of summary health information is shared to obtain premium bids; to modify, amend or terminate a group health plan; or to determine the enrollment or disenrollment status of an individual) or is disclosed pursuant to an authorization. DHHS notes that "because the purpose of the security standards is in part to reinforce privacy protections, it makes sense to align the organizational policies" of the privacy and security rules.

The **required** implementation specifications for this standard are similar to those in the Privacy Rule and call for amending group health plan documents to include provisions requiring the plan sponsor to:

- Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic PHI that it creates, receives, maintains or transmits on behalf of the group health plan.

- Ensure that the adequate separation of electronic PHI required between the group health plan and the plan sponsor is supported by reasonable and appropriate security measures.

- Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information.

- Report to the group health plan any security incident of which it becomes aware.

PHYSICAL STANDARDS AND IMPLEMENTATION SPECIFICATIONS

Facility Access Controls Standard.

Covered entities must implement policies and procedures to limit physical access to their information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. The implementation specifications for this standard are all **addressable** and include:

- Contingency operations, which call for establishing (and implementing, as needed) procedures that allow for facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

- A facility security plan, which calls for implementing policies and procedures to safeguard the facility and the equipment inside of it from unauthorized physical access, tampering and theft.

- Access control and validation procedures, which call for implementing procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision purposes.

- Maintenance records, which call for implementing policies and procedures to document repairs and modifications to the physical components of a facility which relate to security (*e.g.*, hardware, walls, doors and locks).

HMSC Observation. *It is important to recognize that a covered entity is responsible for facility security with respect to protecting electronic PHI, even when it only leases the premises housing such PHI. This duty will require coordination with landlords and/or other tenants. A covered entity also is responsible for extending security standards to members of its workforce wherever they may be working (e.g., at home or off-site), not just on-site.*

Workstation Use Standard.

This standard requires covered entities to implement policies and procedures that specify the proper functions to be performed, how those functions are to be performed and the physical attributes of the surroundings of a specific workstation or class of workstations that can access electronic PHI.

Workstation Security Standard.

Under this standard, covered entities must implement physical safeguards for all workstations that can access electronic PHI. Access must be restricted to authorized users.

Device and Media Controls Standard.

A covered entity must implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI. The standard applies to the receipt and removal of devices and media into and out of a facility and the movement of these items within a facility.

The **required** implementation specifications are to implement policies and procedures:

- For the disposal of devices and media that contain electronic PHI. A device that contains or uses removable media may be subject to this implementation specification in that such removable media must be removed prior to disposal of the device.

- For the removal of electronic PHI from electronic media before that media is made available for re-use.

The **addressable** implementation specifications are to:

- Maintain a record of the movements of hardware and electronic media and any person responsible for the movement.

- Create a retrievable, exact backup of electronic PHI, when needed, before movement of devices.

HMSC Observation. *While some covered entities already have policies and procedures on the removal of electronic and/or other PHI from the covered entity's premises, sign-in and sign-out logs, back-up copies of electronic PHI, disk erasure and hard drive cleansing policies are likely to become more commonplace.*

TECHNICAL STANDARDS AND IMPLEMENTATION SPECIFICATIONS

Access Control Standard.

A covered entity must implement technical policies and procedures that allow access to information systems or related software containing electronic PHI only to persons granted access rights as specified in the information access management standard detailed above.

The **required** implementation specifications for this standard are to:

- Assign a unique name and/or number for identifying and tracking user identity.
- Establish and implement as needed procedures for obtaining necessary electronic PHI during an emergency.

The **addressable** implementation specifications for this standard are to implement:

- Electronic procedures that terminate an electronic session after a predetermined time of inactivity.
- A mechanism to encrypt and decrypt electronic PHI.

Audit Controls Standard.

A covered entity must implement hardware, software and/or procedural mechanisms that record and examine activity in its information systems that contain or use electronic PHI. Electronic "audit trails" will suffice, but DHHS cautions that these audit trails should not be viewed as automatically satisfying the Privacy Rule's accounting requirement for certain disclosures outside of a covered entity.

Integrity Standard.

A covered entity must implement policies and procedures to protect electronic PHI from improper alteration or destruction. The **addressable** implementation specification to this standard is to implement electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner.

Person or Entity Authentication Standard.

A covered entity must implement reasonable and appropriate procedures to verify the authenticity of a person or entity seeking access to electronic PHI.

HMSC Observation. *This standard may be met by the use of electronic signatures although such use is not required.*

Transmission Security Standard.

A covered entity must implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network. Electronic PHI that is being transmitted only needs to be protected in a manner commensurate with the associated risk. For example, encryption may be appropriate for transmission over the Internet.

The **addressable** implementation specifications for this standard are to implement:

- Security measures to prevent electronically transmitted electronic PHI from being improperly modified without detection until disposal.
- A mechanism to encrypt electronic PHI whenever deemed appropriate.

HMSC Observation. *The proposed rule's transmission security standards relating to alarms, audit trails, entity authentication and event reporting of electronic transmissions have been deleted. Although no particular or minimum encryption standard is specified in the Security Rule, the need and level of encryption (as determined by the covered entity) should be reasonable and appropriate for the circumstances. If a covered entity determines that encryption is needed, the encryption should apply to all data, whether during transmission or while stored in memory.*

ORGANIZATIONAL STANDARDS AND IMPLEMENTATION SPECIFICATIONS

Health Care Component Standard.

The Security Rule clarifies that the standards and implementation specifications apply only to the health care components of a hybrid entity. In this regard, the Security Rule tracks the Privacy Rule. Covered entities that are part of larger organizations (that are not themselves covered entities) must ensure that electronic PHI maintained by the covered component is secure from unauthorized access by the other parts of the larger organization, as if the health care component and the other components of the larger organization were separate and distinct legal entities.

Affiliated Covered Entities Standard.

The Security Rule also applies to affiliated covered entities (ACEs). An ACE that performs multiple covered functions, including health care clearinghouse functions, must ensure that the health care clearinghouse component adopts policies and procedures to protect the electronic PHI of the health care clearinghouse from unauthorized access by the other components. Each covered component must comply with the security standards applicable to its respective covered function (*i.e.*, health care provider, health plan or health care clearinghouse).

OTHER STANDARDS

Policies and Procedures Standard.

Covered entities must implement reasonable and appropriate policies and procedures to comply with the Security Rule. Changes to a covered entity's policies and procedures may occur at any time as long as such changes are documented and implemented in accordance with the Security Rule.

Documentation Standard.

Covered entities must maintain in written form (which may be electronic) the policies and procedures they have adopted to comply with the Security Rule. Any action required to be documented by the Security Rule also must be maintained in written form (which also may be electronic). The documentation must be detailed enough to communicate the security measures taken and to facilitate periodic evaluations of a covered entity's compliance with the Security Rule's periodic evaluation standard (discussed above).

The three **required** implementation specifications are that:

- The documentation must be retained for six years from the date of its creation or the date it went into effect, whichever is later.
- The documentation must be available to those persons responsible for implementing the procedures to which the documentation pertains.
- A covered entity must periodically review its documentation and update it as needed in response to changes affecting the security of electronic PHI.

GENERAL CONSIDERATIONS

Preemption.

Although the Security Rule does not address preemption, the Preamble to the Security Rule references the statutory preemption provisions in HIPAA. Based on those provisions, the Security Rule will preempt any contrary state law except for limited exceptions determined by the Secretary of DHHS or mandatory state health plan reporting laws. State or federal laws that provide for more stringent security procedures that are not contrary to the Security Rule are not preempted, and a covered entity must comply with such state and federal laws.

HMSC Observation. *The Preamble discussion of preemption indicates that DHHS seems to believe that the scope of the Security Rule's preemption of state law is greater than that of the Privacy Rule.*

Key Definitions.

The Security Rule has added some useful definitions from the proposed rule and rearranged where other definitions appear. Some key definitions of the Security Rule are:

Electronic Media includes any electronic storage device, such as hard drives or any removable digital memory medium. Electronic media also includes transmission media used to exchange information already in electronic storage media. Examples are the Internet, extranets, private networks and the physical movement of removable electronic storage media. Electronic media does not include facsimiles or vocal telephone communications because the information being exchanged is not in an electronic form before transmission. Video conferencing and voice mail messages also are not included in the definition of electronic media. On the other hand, telephonic voice or keypad response faxback systems (*i.e.*, a request for information from a computer made by voice or telephone keypad input with the requested information returned as a fax) are electronic media.

Electronic Protected Health Information (PHI) generally includes most past, present and future treatment and payment information about a person that is created or received by a covered entity and sent or stored electronically. Electronic PHI also identifies the person who is the subject of the electronic PHI or provides a reasonable basis to do so.

Facility is the physical premises and the interior and exterior of a building.

Information System means an interconnected set of information resources under the same direct management control and that shares common functionality. An information system normally includes hardware, software, information, data, applications, communications and people.

Malicious Software is software that is designed to damage or disrupt a system, such as a virus or a worm.

Security Incident means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information. Security incident also includes interference with system operations in an information system.

Workstation is an electronic computing device or other device that performs similar functions, such as a laptop or desktop computer. A workstation also includes electronic media stored in its immediate environment.

Accessing the Security Rule.

To review the Security Rule in its entirety, click on ***http://law.honigman.com/practice/research.asp?id=8***, or ***http://law.honigman.com/practice/research.asp?id=6***

Honigman Miller Schwartz and Cohn's HIPAA Compliance Team

Honigman Miller Schwartz and Cohn has assembled a HIPAA Compliance Team, led by the attorneys listed below from our Health Care and Employee Benefits Departments, and has developed a number of tools to facilitate compliance. We stand ready to help with any aspect of your compliance planning, from developing a compliance checklist to drafting or reviewing Notices of Privacy Practices, policies, contracts, forms and other documents needed under the Privacy Rule, and assessing legal requirements beyond the Privacy Rule (*i.e.*, state law and other requirements). We would be delighted to answer your questions or otherwise assist you and your colleagues in this important process.

Nicole Bogard	313-465-7398	ndb@honigman.com
Michael Friedman	313-465-7388	mjf@honigman.com
Linda S. Ross	313-465-7526	lsr@honigman.com
Valerie Rup	313-465-7586	vsr@honigman.com
Gregory R. Schermerhorn	313-465-7638	gvs@honigman.com

Honigman Miller Schwartz and Cohn LLP is a general practice law firm headquartered in Detroit, with additional offices in Bingham Farms and Lansing, Michigan. Honigman Miller's staff of more than 175 attorneys and more than 300 support personnel serves thousands of clients regionally, nationally and internationally. Our health care department includes the sixteen attorneys listed below who practice health care law on a full-time or substantially full-time basis, and a number of other attorneys who practice health care law part-time.

William M. Cassetta	Patrick LePine	Chris Rossman
Zachery A. Fryer	Stuart M. Lockman	Valerie Rup
Gerald M. Griffith	Michael J. Philbrick	Julie Schuetze
William O. Hochkammer	Cynthia F. Reaves	Margaret A. Shannon
Ann Hollenbeck	Julie E. Robertson	
Carey F. Kalmowitz	Linda S. Ross	

Our employee benefits department includes the eight attorneys listed below who practice employee benefits law on a full-time basis.

Nicole Bogard	Gregory R. Schermerhorn	Brock E. Swartzle
Michael J. Friedman	Rebecca L. Sczepanski	Lisa B. Zimmer
Mary Jo Larson	Sherill Siebert	

For further information regarding any of the matters discussed in this newsletter, or a brochure that more specifically describes our practices in health care law or employee benefits law, please feel free to contact any of the attorneys listed above by calling our Detroit office at (313) 465-7000, our Bingham Farms office at (248) 566-8300 or our Lansing office at (517) 484-8282.

Honigman Miller Schwartz and Cohn's HIPAA Law Focus is intended to provide information but not legal advice regarding any particular situation. Any reader requiring legal advice regarding a specific situation should contact an attorney. The hiring of a lawyer is an important decision that should not be based solely upon advertisements. Before you decide, ask us to send you free written information about our qualifications and experience. Honigman Miller Schwartz and Cohn also publishes news and client letters concerning antitrust, employee benefits, employment, environmental and tax matters. If you would like further information regarding these publications, please contact Lee Ann Jones at (313) 465-7224, *ljones@honigman.com* or visit the Honigman Miller Schwartz and Cohn website at *www.honigman.com*