Honigman Miller Schwartz and Cohn's *August 2002*

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 MODIFICATIONS TO PRIVACY RULE

Introduction

On August 14, 2002, the United States Department of Health and Human Services (**"DHHS"**) published modifications to the "Standards for Privacy of Individually Identifiable Health Information" (the **"Modifications"**) issued under the Health Insurance Portability and Accountability Act of 1996 (**"HIPAA"**). The Modifications amend the December 28, 2000 Federal Register publication of the "Standards for Privacy of Individually Identifiable Health Information" (the **"2000 Privacy Rule"**) and adopt much of the language contained in the Notice of Proposed Rule Making (**"NPRM"**) issued on March 27, 2002. Additionally, DHHS indicates that it will update the guidance released on July 6, 2001 (**"DHHS Guidance"**) to conform to the Modifications.

The compliance date for the 2000 Privacy Rule, as modified (the **"Privacy Rule"**), is April 14, 2003, except for small health plans for which the compliance date is April 14, 2004. The 2000 Privacy Rule, the NPRM and the Modifications can be found at the Office of Civil Rights' website, *http://www.hhs.gov/ocr/hipaa/*. Also, HMSC has summarized the 2000 Privacy Rule, the NPRM and the DHHS Guidance in previous HIPAA Law Focus newsletters, which can be found at *http://law.honigman.com/knowledge/articles.asp#8*. This edition of HIPAA Law Focus describes the Modifications and their impact on the Privacy Rule.

Consent and Notice of Privacy Practices

In response to concerns that the consent requirements in the 2000 Privacy Rule would interfere with the provision of timely access to quality health care, the Modifications adopt two changes that were proposed in the NPRM. First, the Modifications make obtaining consent to use and disclose protected health information (**"PHI"**) for treatment, payment and health care operations (**"TPO"**) optional on the part of all covered entities, including providers with direct treatment relationships. A covered entity is free to maintain a consent process if it chooses to (or if required by applicable state law). Second, the Modifications strengthen the notice requirements by requiring that direct treatment providers make a good faith effort to obtain a written acknowledgment of receipt of the entity's notice of privacy practices. This change represents DHHS' intent to preserve what it views as a valuable aspect of the consent process, the creation of an "initial moment" between a covered health care provider and an individual, when the parties can focus on and discuss information practices and privacy rights, and when the individual can request restrictions.

DHHS emphasizes that while consent is no longer required, uses and disclosures of PHI for TPO must still be consistent with a covered entity's Notice of Privacy Practices. Additionally, the elimination of the consent requirement has no effect on the requirement for authorizations for uses and disclosures of PHI not otherwise permitted under the Privacy Rule. Thus, while covered health care providers do not need a patient's consent to confer with another provider about the treatment of that patient, the disclosure of PHI from one provider to another for purposes other than TPO may require an authorization.

As noted above, the Modifications require that a covered entity with a direct treatment relationship with an individual make a good faith effort to obtain the individual's written acknowledgment of receipt of the entity's Notice of Privacy Practices. Covered entities without a direct treatment relationship with patients, such as health plans, are not required to obtain this acknowledgment but may choose to do so. DHHS notes that covered entities are provided with broad discretion to design a notice acknowledgment process that works best for their business. The Modifications merely require that the acknowledgment be written. For example, the acknowledgment can appear on the notice itself, on a separate sheet or in a log book.

For persons who refuse to sign or otherwise provide an acknowledgment, covered health care providers must

document their good faith efforts to obtain the acknowledgment and why it was not obtained. A simple statement that the individual refused to sign the acknowledgment will suffice. Failure to obtain the acknowledgment, assuming good faith efforts to do so are documented, is not a violation of the Privacy Rule.

The written acknowledgment should be obtained no later than the date of first service delivery (including services delivered electronically). For emergencies, however, the provision of notice and receipt of a written acknowledgment can be delayed until reasonably practicable after the emergency ends. Additionally, health care providers are exempt from having to make a good faith effort to obtain the individual's acknowledgment in emergency situations. Finally, a new acknowledgment is not required when a Notice of Privacy Practices is changed.

Covered entities must retain a copy of each written acknowledgment of receipt of the Notice of Privacy Practices or documentation of good faith efforts to obtain it. DHHS clarifies that when treatment is not in person (*e.g.*, over the phone), the notice requirement can be met by mailing the notice to the patient on the day of the call and requesting that it be returned with an acknowledgment (*e.g.*, via a tear off sheet). When phone contact is merely for purposes of appointment scheduling, however, the notice and request for acknowledgment can occur at the first patient visit instead. If services are first provided electronically, the acknowledgment should be captured electronically via return receipt or other transmission from the individual.

Finally, DHHS clarifies that it is permissible to have a "layered" Notice of Privacy Practices that includes a summary of the entity's practices followed by a longer detailed description, as long as the Notice of Privacy Practices, taken as a whole, complies with the requirements in the Privacy Rule. DHHS also cautions that while a health plan may arrange to have another entity or person, such as a group administrator or a plan sponsor, distribute the Notice of Privacy Practices on its behalf, the failure of such entity to do so would be a violation of the Privacy Rule by the health plan.

HMSC Observation. *These changes ease some of the burdens on covered entities in complying with the Privacy Rule while creating others. It is important for covered entities to have a good mechanism to document acknowledgments received and good faith efforts to obtain those that are not received. Additionally, although the Privacy Rule no longer requires consent, covered entities may still be subject to consent requirements under state law.*

DHHS notes in several places in the Modifications that the requirement to obtain an individual's acknowledgement not only provides an opportunity for individuals to discuss privacy practices and concerns with their health care providers, but also gives individuals the opportunity to request additional restrictions on uses and disclosures of their PHI. Many covered entities have grappled with policies and procedures for responding to requests for restrictions and the administrative burdens associated with accommodating them. DHHS' emphasis on the right to request restrictions at the juncture of receipt of the notice of privacy practices should cause those covered entities contemplating a policy of either refusing restrictions or accommodating them only in limited circumstances to reconsider that position.

The Modifications provide guidance on how the acknowledgment requirement should be handled in emergency situations. As a practical matter, hospitals may wish to refer to their Emergency Medical Treatment and Active Labor Act compliance policies to determine an appropriate point at which to seek the acknowledgment.

Minimum Necessary Standard

Under the Modifications, all uses and disclosures of PHI made pursuant to a proper authorization are now exempt from the minimum necessary standard. In response to concerns that this change potentially weakens privacy protections, DHHS notes that an individual has the right not to sign an authorization or to negotiate a narrower authorization than requested, and that all authorizations must include a description in a "specific and meaningful fashion" of the information to be used or disclosed. DHHS also states that the Privacy Rule permits, but does not require, a covered entity to use and disclose PHI pursuant to an authorization. The covered entity always may confirm the scope of an authorization with an individual if it has concerns about the type, extent or excessiveness of information requested.

DHHS also clarifies that covered entities must implement criteria designed to limit its non-routine, non-recurring requests for PHI to the minimum necessary to accomplish the intended purposes. For example, if de-identified information can be used to accomplish a particular purpose, the minimum necessary standard dictates use of de-identified

information. Importantly, DHHS instructs that the Privacy Rule allows a covered entity making a disclosure of PHI in response to the request of another covered entity to reasonably rely on the other covered entity's request as being the minimum necessary for the intended disclosure. DHHS also notes, however, that the covered entity always has the discretion to make its own minimum necessary determination.

In other contexts, DHHS notes that the Privacy Rule already exempts from the minimum necessary standard data elements that are required or situationally required in the electronic standard transactions, but that optional elements in those standards would be subject to the minimum necessary standard. Finally, DHHS clarifies that the Privacy Rule is not intended to disrupt existing workers' compensation systems established by state law, and that various provisions in the Privacy Rule permit the disclosures necessary to comply with those laws. DHHS reiterates that the minimum necessary standard does not apply to disclosures required by law.

HMSC Observation. *Although the health care industry is generally relieved that the mandatory consent requirement has been eliminated by the Modifications, it still has concerns that the minimum necessary standard will impede timely access to quality care. The posture of DHHS is that the Modifications are not intended to have this effect and that it will continue to monitor the impact of the consent elimination and consider appropriate revisions to the Privacy Rule as necessary to ensure that timely access to quality care is not impeded. Additionally, the Privacy Rule almost suggests that covered entities have a duty to ensure that not only its own requests are consistent with the minimum necessary standard, but also that requests for disclosures of PHI that it receives are reasonably consistent with the minimum necessary standard. This implicit duty should be addressed in the policies and procedures of covered entities.*

Incidental Uses and Disclosures

The 2000 Privacy Rule did not explicitly address incidental uses and disclosures of PHI occurring as a result of health care communications and practices. The Modifications explicitly permit incidental uses and disclosures of PHI, as long as a covered entity has applied reasonable safeguards and, where applicable, implemented the minimum necessary standard.

An incidental use or disclosure is described as a secondary use or disclosure that reasonably cannot be prevented, is limited in nature and occurs as a by-product of a permitted use or disclosure. Examples of incidental uses and disclosures include using sign-in sheets and calling out patient names in waiting rooms, conferring with medical staff at nurse's stations, talking to patients in semi-private hospital rooms and maintaining bedside patient charts, provided the information used or disclosed is appropriately limited. Additionally, a covered entity is not obligated to isolate x-ray lightboards or destroy empty prescription vials if the covered entity otherwise meets the requirements of the Privacy Rule.

While the existence of an incidental use or disclosure, by itself, does not imply that the covered entity's safeguards are unreasonable, failure to implement reasonable safeguards or, where applicable, the minimum necessary standard is a violation of the Privacy Rule. For example, unimpeded employee access to patient medical records when such employee access is not necessary fails to comply with the minimum necessary standard, and any incidental use or disclosure resulting from this practice is unlawful. Likewise, a physician instructing an office manager to bill a patient for a particular procedure that is overheard by patients in a waiting room is a permissible incidental use or disclosure provided the physician made reasonable efforts to avoid being overheard and reasonably limited the information shared. Incidental uses and disclosures, however, do not excuse erroneous or negligent uses or disclosures, such as sending PHI to the wrong recipient.

HMSC Observation. *While the health care industry requested additional examples of "reasonable safeguards" with respect to incidental uses and disclosures, DHHS does not provide specific guidance due to the differing business needs and circumstances of covered entities. Although DHHS will issue future guidance, it is uncertain as to precisely what constitutes "reasonable safeguards" with regard to making incidental uses and disclosures. These determinations are likely to be made on a case-by-case basis.*

Authorizations

The Modifications retain the consolidated requirements for authorizations that were proposed in the NPRM. The 2000 Privacy Rule required distinct authorizations: (a) for use and disclosure of PHI by the covered entity for its own uses and disclosures, (b) requested by a covered entity for use and disclosure of PHI by others, or (c) for research involving the treatment of the

individual. Now, only a single set of requirements applies to all uses and disclosures that require an authorization, including research.

The Modifications clarify that an individual may not revoke an authorization if the covered entity obtained the authorization as a condition of the individual's receipt of insurance coverage, and other law gives the insurer the right to contest the claim or the insurance policy. The Modifications make the following clarifications as well:

- When an individual initiates an authorization, the purpose for the use and disclosure of PHI may state "at the request of the individual."
- Authorizations need not contain an analysis of the risk of disclosure. Rather, it may include a general statement that the individual's health information may no longer be protected by the Privacy Rule once it is disclosed by the covered entity.
- A covered entity, in its discretion, may state in an authorization that the information will remain subject to the Privacy Rule if the covered entity is requesting the authorization for its own use of PHI.
- The minimum necessary standard does not apply to authorizations.
- Covered entities do not need to account for uses and disclosures made pursuant to an authorization.

Research

The Modifications eliminate the additional requirements for authorizations for the use and disclosure of PHI created for research purposes. Covered entities may combine research authorizations with any other legal permission related to the research study. Significantly, the Modifications remove the requirement for an expiration date for *all* uses and disclosures of PHI for research purposes, but the authorization must contain a statement that the authorization will have no expiration date. Previously, the NPRM provided that the expiration date of the authorization is "at the end of the research study," or "none" when the covered entity uses or discloses PHI solely for the creation or maintenance of a research database or repository.

Although individuals continue to have the right to revoke research authorizations, the Modifications specify that covered entities may continue using and disclosing PHI obtained prior to the revocation as necessary to maintain the integrity of the research study. As with all authorizations, the individual cannot revoke an authorization to the extent a covered entity has acted in reliance upon it.

The Modifications make no changes to the waiver of authorization requirements proposed in the NPRM, as discussed in our HIPAA Law Focus of April 2002. Clarifications relating to research made by the Modifications are:

- By way of a transition period, covered entities may rely on an express legal permission, informed consent or Institutional Review Board (**"IRB"**) approved waiver of informed consent for future unspecified research, as long as the covered entity has obtained permission, the informed consent or the waiver before the compliance date.
- Covered entities do not need a business associate contract to make disclosures to a researcher for research purposes.
- Recruiting individuals to participate in research studies is not a health care operation, and covered entities must obtain an authorization to disclose an individual's information to a third party for this purpose.

Parents and Minors

The general rule under the 2000 Privacy Rule governing the disclosure of health information to parents and guardians about minor children permitted parents to access and control health information about their minor children with limited exceptions set forth in state law. Even when the state law allows minors to consent to treatment without disclosure to a parent or guardian, the 2000 Privacy Rule would have permitted such disclosure where: (a) the minor had agreed to involving the parent or guardian, (b) disclosure was necessary to avert a serious and imminent threat to the health or safety of the minor, and (c) state law had created exceptions to such non-disclosure.

DHHS maintains that this scheme created two areas of uncertainty: (a) where the language of the state law neither prohibited nor permitted disclosure to parents or guardians without the consent of the minor, but instead left it to the provider's discretion, and (b) the rare circumstance where a parent or guardian was not the personal representative of the minor under state law, or where state law was silent or unclear on this point.

To avoid these unintended consequences, DHHS makes two changes. The first change moves the relevant language about the disclosure of a minor's health information to parents or guardians from the definition of "more stringent" into the section directly addressing the standards for personal representatives. The second change adds a new section to clarify the rights of parents to health information about their minor children where they are not the personal representative under state law. This provision establishes a "neutral policy" which provides that a covered entity may provide or deny access to a parent or guardian if such a decision is consistent with state or other applicable law, and the decision is made by a licensed health care professional in the exercise of professional judgment.

HMSC Observation. *These changes seek to avoid the conclusion that the 2000 Privacy Rule imposed greater limitations than imposed by state law on the access right of parents or guardians to health information about their children. These changes are not dramatic, and should not cause any difficulties for covered entities since the "new" general rule is to track what state law already requires. Covered entities already should be familiar with these standards. The emphasis on relying on the professional judgment of health care providers in the absence of bright line rules also should provide additional assurance that in treating adolescents, decisions to disclose or not to disclose to parents or guardians should be defensible.*

Business Associates

The Modifications permit a covered entity to disclose PHI to a business associate that performs a function or activity on its behalf provided that a business associate contract has been executed. In response to industry comments regarding the anticipated administrative cost and burden to renegotiate contracts with business associates, covered entities, excluding small health plans, may continue to operate under certain existing contracts with business associates beyond the April 13, 2003 compliance date. This transition period is available only for preexisting written contracts or agreements that have been in operation prior to October 15, 2002, and that have not been renewed or modified between October 15, 2002 and April 14, 2003.

For purposes of the transition period, contracts that automatically renew without any change in terms or other action by the parties, also known as evergreen contracts, are not deemed a renewal or modification. Likewise, a contract with an automatic inflation adjustment to the price of a contract prior to April 13, 2003 will not be deemed by DHHS as a renewal or modification rendering the contract ineligible for or triggering the end of the transition period. Renewal or modification requires an action by the parties involved.

During the transition period, the covered entity is not relieved of its responsibilities to make information available to the Secretary of DHHS or with respect to an individual's rights of access to, amendment or accounting of his or her PHI. Additionally, the covered entity is obligated to mitigate, to the extent practicable, any harmful effect known to the covered entity relating to a use of disclosure by its business associate. The covered entity, however, is not required to obtain satisfactory assurances from a business associate whose contract is covered by the transition period that the business associate will protect PHI, as discussed in the HMSC HIPAA Law Focus of April 2001.

The Preamble to the Modifications (**"Preamble"**) also clarifies several provisions related to business associate contracts. These clarifications include:

- A business associate contract is not required with persons or organizations whose functions, activities or services do not involve the use or disclosure of PHI and where access to PHI by such persons would be *de minimus*. For example, a business associate contract is not required for janitorial services because these services do not involve the use or disclosure of PHI and, provided reasonable safeguards have been instituted, any contact with PHI would be incidental.
- Disclosures by a covered entity to a researcher for research purposes do not require a business associate contract because research is not a covered function that triggers the business associate requirements.
- No business associate contract is required among members of an organized health care arrangement for their joint activities, such as for centralized billing services.
- A covered entity can delegate its responsibilities to respond to individual requests for access, amendments or accountings to the business associate in the business associate contract.
- A covered entity does not need to provide an individual with access to PHI held by a business

associate if the information held by the business associate is a duplicate of what the covered entity maintains.

- Electronic business associate contracts will satisfy the Privacy Rule requirements provided that an electronic signature will result in a legally binding contract under applicable state law.
- The return or destruction of PHI at the end of a business associate relationship only applies where feasible or permitted by law. Return or destruction is infeasible if other federal or state law requires the business associate to retain the PHI beyond termination of the business associate contract. Where the return or destruction of PHI is not feasible, the business associate contract must state that PHI will remain protected after the contract ends for as long as the PHI is maintained by the business associate.
- DHHS provides sample business associate contract provisions as an appendix to the Modifications. The sample language provided is not required to be in a business associate contract, as long as the contract meets the requirements of the Privacy Rule. Adoption of the sample language does not result in a safe harbor for the covered entity. The sample language does not include other possible contractual elements, such as indemnification, insurance and remedies for breach of contract.

Finally, DHHS anticipates providing technical assistance with respect to the business associate provisions in the future.

HMSC Observation. *Although the Modifications extend the transition period for written contracts or agreements that have not been renewed or modified on or after April 14, 2003, a covered entity may have to negotiate with business associates regarding the handling of individual requests for access, amendments and accountings. These negotiations may result in a modification effectively ending the transition period and requiring compliance with the business associate provisions of the Privacy Rule prior to April 14, 2004.*

De-identification/Limited Data Sets

The Privacy Rule does not apply to PHI that is de-identified by removing 18 enumerated identifiers or by obtaining an expert opinion that a statistically small risk exists that the released information could be used by others to identify the subject of the information. The health care industry expressed concern that the de-identification safe harbor required the removal of many of the data elements essential for research analyses, public health purposes and certain health care operations. In light of these concerns, the Modifications also permit a covered entity to disclose a limited data set if the disclosure is for research, public health purposes or health care operations, and the covered entity obtains a data use agreement from the data recipient.

A limited data set is PHI that excludes 16 identifiers. The two identifiers permitted to be included in a limited data set are: (a) any dates related to the individual, and (b) geographic subdivision, other than street address. Therefore, dates of admission and discharge, dates of birth and death and zip code, county, city or equivalent geocode may be included in a limited data set. Upon removal of the 16 identifiers, the resulting limited data set is not de-identified; it still contains PHI and is subject to the Privacy Rule. Disclosures that include any of the 16 identifiers generally require either the individual's authorization or documentation of an IRB or Privacy Board waiver.

A data use agreement for a limited data set can be combined with a business associate agreement but must:

- Establish the permitted uses and disclosures of the limited data set;
- Limit who can use and receive the limited data set;
- Prohibit use or disclosure of the limited data set other than as permitted by the data use agreement or as otherwise required by law;
- Provide adequate assurances of appropriate safeguards to prevent the use and disclosure of the limited data set in violation of the data use agreement;
- Require the data recipient to report any known use or disclosure that violates the data use agreement to the covered entity;
- Obligate the data recipient to ensure that its agents, including subcontractors, to whom it provides the limited data set agree to the same restrictions and conditions that apply to the data recipient; and
- Prohibit the data recipient from re-identifying the limited data set or contacting the individuals.

As in a business associate agreement, a covered entity may be liable for breach of the data use agreement by the data recipient if it knows of a pattern of activity or

practice that constitutes a material breach of the data use agreement.

HMSC Observation. *The Modifications provide additional flexibility by permitting state hospital associations to conduct and disseminate analyses of health care data and by decreasing the workload of IRBs evaluating waivers of individual authorizations due to the impracticality of using de-identified data. A state hospital association and its member hospitals may be parties to a common data use agreement or include data use provisions with a business associate agreement.*

Marketing

In the NPRM, DHHS hoped to simplify and clarify the rules relating to marketing by distinguishing health care communications from marketing functions. The Modifications adopt the NPRM substantially as proposed, but make changes to the proposed definition of "marketing" and further clarify certain exclusions from the definition of marketing. The Modifications change the definition of marketing as follows:

- The Modifications eliminate the special provisions for marketing health-related products and provide that a covered entity must have an individual's prior written authorization to use or disclose PHI for marketing communications. No longer will covered entities be able to use such information by meeting the disclosure and opt-out provisions previously established in the 2000 Privacy Rule.
- The definition of marketing, as refined, now reads: "to make a communication about a product or service that encourages the recipients of the communication to purchase or use the product or service." The use of the term "that encourages" rather than "to encourage" reflects DHHS' decision to determine whether a communication is "marketing" based solely on the face of communication, rather than on a subjective determination of the sender's intent.
- A covered entity is not engaged in "marketing" when it communicates to individuals about: (a) the participating providers and health plans in a network, the services offered by a provider, or the benefits covered by a health plan, (b) the individual's treatment, or (c) case management or care coordination for that individual, or directions or recommendations for alternative treatments, therapies, health care providers, or settings of care to that individual. For example, a doctor who writes a prescription or refers an individual to a specialist for follow-up tests is engaging in a treatment communication and is not marketing a product or service.
- DHHS specifically broadens the NPRM proposed language by allowing covered entities to convey information to beneficiaries and members about health insurance products offered that could enhance or substitute for existing health plan coverage. This exception does *not* apply to certain excepted benefits, such as other lines of insurance offered by the covered entity or when such communications are not benefits to a covered entity's membership, but constitute merely pass-through benefits available to the public at large.
- The Modifications close a perceived loophole that a covered entity could sell PHI to another company for the marketing of that company's products or services through a business associate contract. "Marketing" now includes "an arrangement between a covered entity and any other entity whereby the covered entity discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service."
- The Modifications require an authorization for uses and disclosures of PHI for marketing communications except: (a) when the communication occurs in a face-to-face encounter between the covered entity and the individual, or (b) where the communication involves a promotional gift of nominal value.

Finally, DHHS clarifies that nothing in the marketing provisions of the Privacy Rule are to be construed as amending, modifying, or changing any rule or requirement related to any other federal or state statutes or regulations, including specifically anti-kickback, fraud and abuse, or self-referral statutes or regulations, or to authorize or permit any activity or transaction currently proscribed by such statutes and regulations. The definition of "marketing" is intended solely to apply to the Privacy Rule, and the authority granted by the Privacy Rule is only for a covered entity's use or disclosure of PHI.

HMSC Observation. *The adoption of the NPRM exclusion from the definition of marketing of certain health treatment communications is a reasonable and welcome clarification in the Privacy Rule. Absent these clarifications, routine health communications would have been stymied. The Preamble to the Modifications states that: (a) a doctor who writes a prescription or refers an individual to a specialist for follow-up tests is engaging in a treatment communication and is not marketing a product or service, (b) a health plan would not be considered to be engaging in marketing when it advises its enrollees about other available health plan coverages that could enhance or substitute for existing health plan coverage, and (c) for a child about to age out of coverage under a family's policy, the plan can send the family information about continuation coverage for the child. Note that this exception would not allow for the marketing of unrelated lines of insurance based upon the use of PHI.*

The Modifications remove from the definition of marketing any communications related to treatment, even if a covered entity receives remuneration for those communications. Arguably, a covered entity would not violate the Privacy Rule by recommending one product or service over another among a group of competing products and services, even if it receives remuneration for doing so. Consumers objecting to these practices may take action under other consumer protection statutes of federal agencies, such as the Federal Trade Commission. Additional guidance, and perhaps legislation, is likely in these areas.

Although the Privacy Rule defines the term "marketing" to exclude communications to an individual to recommend, purchase, or use a product or service as part of the treatment of the individual or for case management or care coordination of that individual, such communication by certain health care providers, such as physicians, may violate state and federal anti-kickback statutes. Clients should insure that, in this regard, that their compliance solutions under the Privacy Rule do not violate the anti-kickback and Stark Law prohibitions. For example, a pharmacist's communications with patients relating to the marketing of products on behalf of pharmaceutical companies were identified by the Office of Inspector General as problematic, while such communications do not constitute marketing under the Privacy Rule.

Accountings

The Modifications expand the categories of disclosures that are not subject to accountings. Perhaps most significantly, covered entities no longer must account for disclosures made pursuant to valid authorizations. DHHS' rationale is that the authorization process itself adequately protects the individual's privacy by assuring that any authorization is provided both knowingly and voluntarily.

Two other categories of disclosures also are excluded from the accounting requirement: (a) disclosures of information that are part of a limited data set, and (b) disclosures that are "incidental" to other permissible uses and disclosures. Thus, the Privacy Rule now exempts the following disclosures from the accounting requirement: (a) disclosures for TPO purposes, (b) disclosures to individuals of their own PHI, (c) permitted incidental disclosures, (d) disclosures pursuant to a valid authorization, (e) disclosure's for a facility directory or to persons involved in the individual's care, (f) disclosures for national security or intelligence purposes, (g) disclosures to correctional institutions or law enforcement officials, (h) disclosures that are part of a limited data set, and (i) disclosures that occurred prior to the compliance date for the covered entity.

In addition, covered entities may now account for research disclosures made pursuant to a waiver of authorization by providing individuals with a list of all protocols for which the patient's PHI may have been disclosed, as well as the researcher's name and contact information. This simplified procedure is available in cases where the research disclosure contains records of at least 50 individuals, thus justifying the simplified procedure. When requested by the individual, the covered entity must help to contact the researchers to whom the individual's PHI was actually disclosed.

Finally, DHHS keeps the requirement of accounting for public health disclosures and emphasizes that a covered entity has a responsibility with respect to accounting for requests for disclosures relating to victims of domestic abuse, neglect or domestic violence. If individuals insist on an accounting even after being warned of the potential dangers, the covered entity must comply, but if the covered entity has a reasonable belief that the requesting party is the abuser, it has the discretion to decline the request.

HMSC Observation. *These changes simplify the task of accounting for disclosures; however, not all incidental disclosures are "permitted." If a covered*

entity does not take reasonable precautions to prevent an incidental disclosure (including adhering to the minimum necessary standard) then any such disclosure is not permitted and is subject to the accounting requirements. This underscores the need for reasonable safeguards and complying with the minimum necessary standard.

Additionally, because only disclosures pursuant to valid authorizations are exempt, covered entities will also have to be diligent about obtaining, enforcing authorizations, and maintaining the ability to track revocations of authorizations. Otherwise, they may be required to account for improperly authorized disclosures mistakenly believed to be exempt.

Group Health Plans: Disclosures of Enrollment and Disenrollment Information

The Modifications add a new section that clarifies that a group health plan, or an insurer or health maintenance organization (**"HMO"**) providing benefits with respect to a group health plan, may disclose to the plan sponsor whether an individual is a participant in the group health plan, or has enrolled or disenrolled in the coverage provided by the insurer or HMO, without the plan sponsor having to amend the plan documents to provide for such disclosure.

Thus, there are now two circumstances, under the Privacy Rule, when a group health plan may share information with the plan sponsor without an individual's authorization and without an amendment to the plan documents. The first is the provision of summary health information (*i.e.*, information that does not contain the 18 specified identifiers and that is given to employers for the limited purposes of soliciting insurance premium bids or providing cost data for the employer to decide whether to amend or terminate its group health plan), and the second is the enrollment/disenrollment information just noted.

The Preamble also clarifies that the exceptions to the notice and the administrative requirements for fully insured health plans apply if the only information provided to the plan sponsor by the plan, the insurer or the HMO is summary health information and information about the participation and/or enrollment/disenrollment status of individuals. The Privacy Rule does not define the information that may be transmitted for enrollment/disenrollment purposes, but does reference the medical information data elements (*e.g.*, height, weight, substance/tobacco abuse, *etc.*) in the electronic standard transaction for enrollment/disenrollment. DHHS clarifies in the Preamble that any medical information provided to the plan sponsor beyond those data elements would take even a fully insured group health plan out of these exceptions, (*i.e.*, it would no longer be able to rely on the insurer's or HMO's compliance with the Privacy Rule, but would have to comply on its own.)

One other change noted in the Preamble affecting group health plans and their employer sponsors is a clarification in the definition of "required by law" as including a law that compels any entity, not just covered entities, to make a use or disclosure of PHI. This clarification is intended to protect employers, who are not covered entities, in those circumstances when applicable law requires them to disclose medical information about employees (*e.g.*, Office of Safety and Health Administration or comparable state laws).

HMSC Observation. *Because employer/plan sponsors are not covered entities, they are not required to submit enrollment/disenrollment information to their group health plans, or the insurers and/or HMOs providing benefits under their group health plans, in compliance with the electronic standards. Nothing in the Modifications changes that. Employers may, of course, voluntarily elect to comply with the electronic transaction standards if requested to do so by their insurers or HMOs, and if they do, would likely enter into a trading partner agreement defining the scope of their contractual obligation.*

Many plan sponsors, however, receive regular reports from their insurers and HMOs about the claims experience of their workforce and their dependents. Those employers wishing to fit their group health plan into the Privacy Rule's compliance exception for fully insured plans, must evaluate what information is currently included in those reports, to what extent it is "individually identifiable," and whether they can meet their budgeting and cost monitoring needs with the degree of limited information that is required to come within the exception. Employers who fully insure their group health plans should not simply assume that those plans can avoid having to independently comply with the Privacy Rule, but instead can rely on the efforts of their insurers and/or HMOs.

Employment Records

The Modifications adopt the proposed language in the NPRM excluding employment records from the definition of PHI. DHHS declines to provide a definition of employment records. The Modifications,

however, specify that medical information needed for an employer to fulfill its responsibilities under the Family Medical Leave Act, Americans with Disabilities Act (**"ADA"**) and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance and fitness-for-duty test of employees, may be part of an individual's employment records, and nothing in the Privacy Rule prevents employers from obtaining this information.

HMSC Observation. *Other federal and state laws (e.g., the ADA) may require an employer to separate this medical information from the employee's general personnel file, and these laws still apply. Moreover, while some medical information that employers obtain about their employees is not subject to the Privacy Rule, this only means that employers cannot be penalized for violating the Privacy Rule for disclosing medical information that is not PHI. Employers should be aware, however, that the standards established by the Privacy Rule may well become the de facto standard of care for protecting confidential medical information for purposes of state tort litigation. Although not required, it might nevertheless be wise for employers to treat all confidential medical information about employees and their families as if it were PHI.*

Disclosures for TPO of Other Entities

The Modifications adopt the NPRM proposal to allow a covered entity to disclose PHI for the TPO of another entity as follows: (a) a covered entity may use or disclose PHI for the treatment activities of any health care provider (whether or not that provider is a covered entity), (b) a covered entity may disclose PHI to another covered entity or any health care provider for the payment activities of the entity that receives the information, and (c) a covered entity may disclose PHI to another covered entity for the health care operations activities of the entity that receives the information. In the latter circumstance, a covered entity may only disclose PHI to another entity if each entity either has or had a relationship with the individual who is the subject of the PHI, the PHI pertains to that relationship, and the disclosure is for health care operations (*e.g.*, quality assessment, case management and care coordination, accreditation, licensing, or credentialing activities, *etc.*); or for the purpose of health care fraud and abuse detection or compliance.

A covered entity that participates in an organized health care arrangement may disclose PHI about an individual to another covered entity that participates in the organized health care arrangement for any health care operations activities of the organized health care arrangement. The covered entity in this circumstance need not have a current relationship with the recipient of the PHI (*e.g.*, when a group health plan needs PHI from a former insurer).

HMSC Observation. *The Modifications add flexibility for covered entities to communicate among one another for TPO. The Preamble clarifies that "payment" includes uses and disclosures necessary for coordination of benefits purposes and disclosures to obtain payment under a reinsurance contract.*

Hybrid Entities

The Modifications grant covered entities the discretion to decide whether to be a hybrid entity. As a result, the proportion of the covered entity's covered functions to its non-covered functions is no longer a factor in determining its eligibility for hybrid entity status. Any covered entity that otherwise qualifies (*i.e.,* it is a single legal entity that performs both covered and non-covered functions) and that designates its health care component(s) can be a hybrid entity.

A covered entity that elects hybrid entity status has discretion to select what functions are to be included in its health care component. A hybrid entity may include in its health care component a non-covered health care provider component and business associate divisions. A hybrid entity that chooses to include a non-covered health care provider in its health care component is required to ensure that the non-covered health care provider, as well as the rest of the health care component, complies with the Privacy Rule. Covered entities that choose not to designate health care component(s) are subject to the Privacy Rule in their entirety.

HMSC Observation. *A covered entity now has the flexibility to apply the hybrid entity provisions of the Privacy Rule as best suited to its organizational structure. It is important for a covered entity to weigh the pros and cons of electing hybrid entity status, with its consequent division into health care components and other components.*

Uses and Disclosures for Food and Drug Administration ("FDA") purposes

The Modifications permit covered entities to disclose PHI without authorization to a person subject to the jurisdiction of the FDA for public health purposes relating to the quality, safety or effectiveness of FDA-regulated products or activities, such as collecting or reporting adverse events, dangerous products, and defects or problems with FDA-regulated products. Persons subject to FDA jurisdiction include pharmaceutical and medical device manufacturers, providers of biological products (*e.g.*, blood and tissue products), and their representatives. The minimum necessary standard applies to these disclosures and disclosures must be for a valid public health purpose; disclosures for commercial purposes are not permitted.

Changes in Legal Ownership

DHHS clarifies that the definition of health care operations includes not only due diligence activities related to a sale, transfer, merger or consolidation, but also the actual transfer of PHI in connection with the consummation of the transaction. Prior to these clarifications, due diligence activities were deemed part of health care operations, but there was no provision allowing for the actual transfer of PHI as part of the transaction. Additionally, the term health care operations in the 2000 Privacy Rule was limited to sale or merger transactions and did not include transfers and consolidations. Significantly, DHHS clarifies that any disclosures for these purposes must be made by the covered entity that is a party to the transaction. In the new owner's hands, the PHI remains subject to the protections of the Privacy Rule. Thus, authorizations still are required for uses and disclosures of the PHI not otherwise permitted without authorization under the Privacy Rule. Finally, in response to comments expressed about transactions that are not consummated after PHI is exchanged in the due diligence process, DHHS notes that other laws and business practices (*e.g.*, confidentiality agreements) adequately address these circumstances.

HMSC Observation. *Only covered entities are authorized to provide PHI to others in connection with due diligence and the underlying transaction. Thus, while not explicit in the Privacy Rule, covered entities should be responsible for coordinating the flow of PHI in the due diligence process to ensure that the covered entities are the source of the information. Additionally, covered entities should routinely enter into confidentiality agreements calling for the return of all PHI provided in the due diligence process in the event that the transaction is not consummated. One question left open by the Modifications is whether the definition of health care operations encompasses due diligence and transfer of PHI in the context of joint ventures, joint operating agreements and other affiliations that are not sales, mergers, transfers or consolidations.*

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 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
Cynthia F. Reaves	313-465-7686	cfr@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
Zachery A. Fryer
Gerald M. Griffith
William O. Hochkammer
Ann Hollenbeck
Carey F. Kalmowitz
Patrick LePine
Stuart M. Lockman
Michael J. Philbrick
Cynthia F. Reaves
Julie E. Robertson
Linda S. Ross
Chris Rossman
Valerie Rup
Julie Schuetze
Margaret A. Shannon

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

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

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 web site at www.honigman.com