HHS has issued a notice of proposed rules which, if finalized, will modify the HIPAA Privacy, Security and Enforcement Rules. The purpose of the proposed modifications is to implement recent statutory amendments under the Health Information Technology for Economic and Clinical Health Act ("the HITECH Act").[1] Subjects not addressed by these rules include the accounting for disclosures requirement or the penalty distribution methodology requirement which will be the subject of future rulemakings.

Covered entities and business associates will have 180 days after the effective date of the final rule to come into compliance with most of the rule's provisions unless a different compliance period is expressly provided for in the regulation. Moreover, modifications to the provisions of the HIPAA Enforcement Rule are in effect and apply at the time the final rule becomes effective or as otherwise specifically provided as such provisions are not standards or implementation specifications.

Although passage of the HITECH Act requires most of the proposed modifications, it does not account for all of the proposed changes. Indeed, the Department is taking the opportunity to eliminate ambiguities and improve the workability and effectiveness of all three sets of HIPAA Rules which have not been substantially amended in years – Privacy Rule has not been amended since 2002, Security Rule since 2003 and Enforcement Rule since 2006 (although it was slightly amended in 2009).

GENERAL PROVISIONS WHICH APPLY TO ALL HIPAA RULES

The modifications would make clear that the HIPAA Rules apply to business associates, where so provided. Moreover, the definition of who is considered a "business associate" would be expanded and the definition would be clarified with respect to the circumstances when a business associate relationship exists. Specifically, Patient Safety Organizations performing patient safety activities for a

[1] HITECH modifies certain provisions of the Social Security Act pertaining to the Administrative Simplification Rules (HIPAA Rules) and requires certain modifications to the HIPAA Rules themselves.

covered entity will give rise to a business associate relationship. Also included are Health Information Organizations, E-prescribing Gateways and others that (a) provide data transmission of protected health information to a covered entity (or its business associate), and (b) require access on a ***routine basis*** to such protected health information; and, vendors that contract with a covered entity to provide personal health records to patients on behalf of the covered entity. Finally, "subcontractors," agents or other persons who perform functions for or provide services to a business associate, other than in the capacity as a member of the business associate's workforce, and require access to protected health information, are considered business associates.

The intent of including "subcontractors" as individuals requiring business associate agreements is to avoid having privacy and security protections for protected health information lapse merely because a function is performed by an entity that is a subcontractor rather than an entity with a direct relationship with a covered entity.

SECURITY RULE

Again, proposed modifications to the security rule makes clear that the rules apply to business associates as well as subcontractor's of business associates who create, receive, maintain or transmit protected health information on behalf of a business associate. However, the proposed modification is not intended to mean that a covered entity is required to have a contract with the subcontractor. Instead, the obligation remains with the business associate who contracts with the subcontractor to obtain the required satisfactory assurances from the subcontractor to protect the security of electronic protected health information. Moreover, the contract between the business associate and its subcontractor must require the subcontractor to report any security incident to which it becomes aware to the business associate. The business associate must then notify the covered entity of the breach and,

unless such function has been delegated to the business associate, the covered entity must notify the affected individuals, the Secretary and, if applicable, the media, of the breach.

PRIVACY RULE

Marketing

The Privacy Rule requires covered entities to obtain a valid authorization from individuals before using or disclosing protected health information to market a product or service to them. The proposed modifications alter the definition of "marketing" in response to the HITECH Act's limits on the types of health-related communications that may be considered health care operations and thus, that are excepted from the definition of "marketing" under the Privacy Rule to the extent a covered entity receives or has received direct or indirect payment in exchange for making the communication. The HHS believes Congress intended with these HITECH provisions to curtail a covered entity's ability to use the exceptions to the definition of "marketing" in the Privacy Rule to send communications to the individual that were motivated more by commercial gain or other commercial purpose rather than for the purpose of the individual's health care, despite the communication's being about a health-related product or service. To implement the marketing limitations of the HITECH Act, the proposed modifications to the definition of "marketing" include: (1) revise the exceptions to marketing to better distinguish the exceptions for treatment communications from those communications made for health care operations; (2) add a definition of "financial remuneration;" (3) provide that health care operations communications for which financial remuneration is received are marketing and require individual authorization; (4)provide that written treatment communications for which financial remuneration is received are subject to certain notice and opt out conditions; (5) provide a limited exception from the remuneration prohibition for refill reminders; and (6) remove the paragraph regarding an arrangement

between a covered entity and another entity in which the covered entity receives remuneration in exchange for protected health information.

Although the intent with respect to the definition of "marketing" is to maintain the general concept that "marketing" means "to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service," the proposed modifications include three exceptions to the definition to encompass certain treatment and health care operations communications about health-related products or services.

The first exception proposed is to exclude certain health care operations communications, except where, the covered entity receives financial remuneration in exchange for making the communication. The proposed definition of "financial remuneration" includes direct or indirect payment from or on behalf of a third party whose product or service is being described but does not include any direct or indirect payment for the treatment of an individual. In addition, the financial remuneration must be in exchange for making the communication itself and be from or on behalf of the entity whose product or service is being described. For example, authorization would be required prior to a covered entity making a communication to its patients regarding the acquisition of new state of the art medical equipment if the equipment manufacturer paid the covered entity to send the communication to its patients. In contrast, an authorization would not be required if a local charitable organization (such as a breast cancer foundation) funded the covered entity's mailing to patients about the availability of new state of the art medical equipment (such as mammography screening equipment) since the covered entity would not be receiving remuneration by or on behalf of the entity whose product or service was being described. Also, authorizations would not be required if a hospital sent flyers to its patients announcing the opening of a new wing where the funds for the new wing were

donated by a third party, since the financial remuneration to the hospital from the third party was not in exchange for the mailing of the flyers.

The second proposed exception to "marketing" is for communications regarding refill reminders or otherwise about a drug or biologic that is currently being prescribed for the individual, provided any financial remuneration received by the covered entity for making the communication is reasonably related to the covered entity's cost of making the communication.

The third proposed exception to "marketing" are treatment communications about health-related products or services by a health care provider to an individual, including communications for case management or care coordination for the individual, or to direct or recommended alternative treatments, therapies, health care providers, or settings of care to the individual, provided, however, that if the communications are in writing and financial remuneration is received in exchange for making the communications, certain notice and opt out conditions are met. To insure the individual is aware that he or she may receive subsidized treatment communications from his or her provider and has the opportunity to elect not to receive them, the proposed modifications would require a statement in the notice of privacy practices when a provider intends to send such subsidized treatment communications to an individual, as well as the opportunity for the individual to opt out of receiving such communications. Specifically, the proposed rule would exclude from marketing and the authorization requirements written subsidized treatment communications only to the extent that the following requirements are met: (1) the covered health care provider's notice of privacy practices includes a statement informing individuals that the provider may send treatment communications to the individual concerning treatment alternatives or other health-related products or services where the provider receives financial remuneration from a third party in exchange for making the communication, and the individual has a right to opt out of receiving such communications; and (2) the treatment

communication itself discloses the fact of remuneration and provides the individual with a clear and conspicuous opportunity to elect not to receive any further such communications. The opt out method should not cause the individual to incur an undue burden or more than a nominal cost.

Importantly, it is noted that face to face communications about products or services between a covered entity and an individual and promotional gifts or nominal value provided by a covered entity are not impacted by these proposed changes to the definition of "marketing." Neither are communications made by covered entities to individuals promoting health in general or communications about government and government-sponsored programs.

Business Associates

As HITECH made clear that the Privacy Rules apply to business associates just as they apply to covered entities, proposed modifications to the Privacy Rules include revisions to provide that a business associate, like a covered entity, may not use or disclose protected health information except as permitted or required by the Privacy Rule or the Enforcement Rule. Moreover, proposed modifications would allow business associates to use or disclose protected health information only as permitted or required by their business associate contracts or other arrangements or as required by law. If a covered entity and business associate have failed to enter into a contract or other arrangement, then the business associate may use or disclose protected health information only as necessary to perform its obligations for the covered entity or as required by law.

Moreover, the proposed modifications revise the minimum necessary standard to require that when business associates use, disclose, or request protected health information, they limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Like the proposed modifications to the Security Rule, the proposed modifications to the Privacy Rule require the business associate to enter into a contract or other arrangement with business associate subcontractors, this will not be the responsibility of the covered entity. Moreover, business associates and business associate subcontractors would have direct liability under the HIPAA Rules.

Business Associate Agreements

There are several proposed modifications to business associate agreements: (1) remove the requirement that covered entities report to the Secretary when termination of a business associate contract is not feasible; (2) add a requirement that a business associate must cure a subcontractor breach or terminate the contract, if feasible, due to noncompliance by the subcontractor; (3) require that business associates comply, where applicable, with the Security Rule with regard to electronic protected health information; (4) require that business associates report breaches of unsecured protected health information to covered entities; (5)require that business associates ensure that any subcontractors that create or receive protected health information agree to the same restrictions and conditions that apply to the business associate with respect to the information; (6) add a requirement that to the extent a business associate is to carry out a covered entity's obligation, the business associate must comply with the requirements of the Privacy Rule that apply to the covered entity in the performance of such obligation or be subject to direct liability. These proposed modifications would also apply to the contracts or other arrangement entered into between business associates and subcontractors .

In an attempt to relieve some of the burden on covered entities and business associates in complying with the revised business associate agreement provisions, a proposed transition period is suggested to grandfather in certain existing contracts for a specified period of time. Parties can continue to operate under existing contracts for up to one year beyond the compliance date of the

revisions to the Rules if, prior to the publication date of the modified Rules, the covered entity or business associate had an existing contract or other written arrangement with a business associate or subcontractor, respectively, that complied with the prior provisions of the HIPAA Rules and such contract or arrangement was not renewed or modified between eh effective date and the compliance date of the modifications to the Rules.

Authorizations

Currently, the Privacy Rule permits a covered entity to use and disclose protected health information only if it has obtained a valid authorization unless such use is otherwise permitted but specifically requires authorizations for (1) most uses and disclosures or psychotherapy notes; and (2) uses and disclosures for marketing. The proposed modifications would add a third: the sale of protected health information. In these circumstances, the authorization must state that the disclosure will result in remuneration to the covered entity. There are several proposed exceptions to this authorization requirement : exchanges for remuneration for public health activities; disclosures for research purposes; disclosures for treatment and payment purposes in which the covered entity receives remuneration; disclosures for the sale, transfer, merger, or consolidation of all or part of a covered entity with another covered entity; disclosures to or by a business associate for acts on behalf of a covered entity as long as the only remuneration provided is by the covered entity to the business associate for the performance of such activities; disclosures by a covered entity to an individual when requested by the individual; and, disclosures required by law.

The proposed modifications to the Rules would revise the period of protection for a decedent's information – a covered entity would only be required to comply with the requirements of the Privacy Rule for a period of 50 y ears following the date of death. In addition, a proposed amendment would permit covered entities to disclose a decedent's information to family members and others who were

involved in the care or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

Under the proposed modifications, covered entities can disclose proof of student immunization to schools in States that have school entry or similar laws, without written authorization, but with oral agreement from the parent or guardian.

Minimum Necessary Requirement

With respect to the Privacy Rule's "minimum necessary" requirement – that covered entities limit uses and disclosures of, and requests for, protected health information to "the minimum necessary to accomplish the intended purpose of the use, disclosure, or request," the Department is not making any modifications but, instead, is soliciting public comment on how the Department can determine the minimum necessary for purposes of complying with the Privacy Rule.

Notice Of Privacy Practices For Protected Health Information.

Under the proposed modifications, covered entities will be required to make "material modifications" to their Notice of Privacy Practices ("Notice") therefore triggering obligations to revise and distribute the "new" Notices. For example, covered entities will have to revise their Notices consistent with new changes to the patient rights portion of the rule. Specifically, although the current rules allow a covered entity to decline to accept a patient's request for restrictions as stated in the Notice, the proposed rules require a covered entity to agree to a patient's request not to disclose protected health information to a health plan if the purpose of the disclosure to the plan is for carrying out payment or health care operations and the protected health information pertains solely to health care services for which the patient or, another person on behalf of the patient, has paid the covered entity in full. In other words, a patient can restrict a health care provider from disclosing protected

health information to the patient's health plan as long as the patient pays out of pocket for the service in full. Importantly, if the patient's payment is not honored (e.g., the check bounces), the provider is permitted to submit the protected health information to the health plan in order to be paid for the service. The health care provider need only comply with the restriction for services in which the provider is paid in full. The Office of Civil Rights ("OCR") makes clear that it does not believe that the intent of the HITECH ACT was to allow patients to avoid their payment obligations to health care providers. The proposed regulations also would require changes to the Notice regarding notifying patients which uses and disclosures require an authorization. The proposed rules would also require covered entities to disclose to patients that most disclosures for protected health information for which the covered entity receives remuneration require authorization. The Notice will also have to be revised to reflect the new requirements concerning marketing and subsidized treatment communications. The OCR is also soliciting comments on whether the Privacy Rule should require that the Notice contain a required statement advising patients of the new breach notification obligations with respect to breaches of unsecure information.

Notably, the OCR states that the change to the existing patient rights rule and other changes noted above are "material" thus requiring all covered entities who have Notice obligations to revise their Notices and reissue them. This means that although the handing out of a Notice to a patient is typically a one-time obligation (i.e., continuing patients need not be offered a Notice at every visit), the provider will now have to ensure that all patients are provided a new Notice at their next visit and maintain a copy of the patient's acknowledgment that they have been given a copy of the new Notice. Many providers have not revised their Notices since inception of the Privacy Rule and thus have not had the burden of providing all existing and continuing patients with new Notices. Importantly for health plans, the OCR recognizes that revising and redistributing Notices within 60 days of material changes for

health plans is a costly process and thus the OCR is seeking comments on ways in which plans could inform individuals of the changes without imposing a large burden. The OCR is considering many options such as replacing the current 60 day requirement with a requirement that the plan redistribute the new Notice in the next annual mailing such as at the beginning of the plan year or during the open enrollment period and is also considering whether it should make no changes. Obviously, it is in the best interest of plans to proactively comment to the OCR on this important issue.

Right To Request Restriction Of Uses And Disclosures.

A new section is proposed to require covered entities, upon request from an individual, to agree to a restriction on the disclosure of protected health information to a health plan or to a business associate of the health plan if: (A) the disclosure is for the purposes of carrying out payment or healthcare operations and is not otherwise required by law; and (B) the protected health information pertains solely to a health care item or service for which the individual, or person on behalf of the individual other than the health plan, has paid the covered entity in full. This modification would override the current provision that states that a covered entity is not required to agree to requests for restrictions which would have to be modified accordingly.[2] With respect to this modification, the Department makes clear that it does not believe that a covered entity could require individuals who wish to restrict disclosures about only certain health care items or services to a health plan to restrict disclosures of protected health information regarding all health care to the plan – i.e., to require an individual to have to pay out of pocket for all services to take advantage of this right regardless of the particular health care item or service about which the individual requested the restriction. Allowing a covered entity to do so, according to the Department, would be contrary to Congressional intent, in that it would discourage individuals from requesting restrictions in situations where Congress clearly

[2] The proposed modification would permit a covered entity, however, to disclose protected health information to a health plan if such disclosure is required by law, despite an individual's request for a restriction. Comment is requested on examples of types of disclosures that may fall under this provision.

intended they be able to do so. As the Department recognizes that this provision may be more difficult to implement in some circumstances than in others, it has requested comment on the types of interactions between individuals and covered entities that would make requesting or implementing a restriction more difficult. In addition, the Department asks for comment on three specific issues : (1) how a provider, who uses an automated electronic prescribing tool, could alert the pharmacy that the individual may wish to request that a restriction be placed on the disclosure of their information to the health plan and that the individual intends to pay out of pocket for the prescription and, (2) what the obligation is, if any, of covered health care providers that know of a restriction to inform other health care providers downstream of a requested restriction; and, (3) the extent to which technical capabilities exist that would facilitate notification among providers of restrictions on the disclosure of protected health information, how widely these technologies are currently utilized, and any limitations in the technology that would require additional manual or other procedures to provide notification of restrictions.

The Department does question how this provision will function with respect to HMOs as a provider generally receives a fixed payment from an HMO based on the number of patients seen and an individual patient of that provider pays a float co-payment for every visit regardless of the treatment or service received. Thus, it does not appear that with an HMO situation, an individual could pay the provider for the treatment or service rendered and may have to use an out-of-network provider if they wish to ensure that certain protected health information is not disclosed to the HMO. The Department requests comment on this issue.

Finally, the Department emphasizes that if an individual's payment for a health care item to restrict disclosure is not honored (for example, the check bounces), the covered entity may then submit the information to the health plan for payment as the individual has not fulfilled the requirements

necessary to obtain a restriction. However, it is expected that covered entities will make reasonable attempts to resolve the payment issue with the individual prior to sending the information to the health plan and requests comment on this issue.

The final issue is termination of the restriction. If an individual asks the provider to bill the health plan for follow-up treatment involving the condition which the individual initially requested a restriction on, the provider may need to submit information about the original treatment to the health plan in order to secure payment. In this case, the Department would consider the lack of a restriction with respect to the follow-up treatment to extent to any protected health information necessary to effect payment for such treatment, even if such information pertained to prior treatment that was subject to a restriction. The Department encourages covered entities to have an open dialogue with individuals to ensure that they are aware that protected health information may be disclosed to the health plan and asks for comment on this issue.

Access Of Individuals To Protected Health Information.

The proposed modifications expand a covered entities obligations with respect to providing access to individuals of their protected health information. Under the proposed rules, if the protected health information requested is maintained electronically in one or more designated record sets, the covered entity must provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. This provision would require a covered entity to provide the information in electronic form if it maintains the information electronically. Since there are covered entities which are not technologically mature and do not maintain the requested information electronically, these covered entities may make some other agreement with individuals to provide a readable electronic copy (i.e., PDF copy). This modification

presumes that covered entities have the capability of providing electronic copies securely but invite comment and this assumption.

The modifications also expand the current requirement that a covered entity provide access in a *timely manner* in providing that, if requested by an individual, a covered entity must transmit the copy of protected health information directly to another person designated by the individual. However, the individual's choice must be "clear, conspicuous, and specific" which is secured by requiring that the individual's request by "in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information." The request can be electronic or paper-based, however, a covered entity must implement reasonable policies and procedures to verify the identity of the requesting individual.

Finally, the Department has requested comment on whether a single timeliness standard should be adopted for the provision of access or if a variety of timeliness standards based on the type of electronic designated record set is the preferred approach. Under either approach, comment is sought as to proposed reasonable timeframe(s) or comment on whether the current standard could be altered for all systems, paper and electronic, such that all requests for access should be responded to without unreasonable delay and not later than 30 days. Comment is also sought on the time necessary for covered entities to review access requests and make necessary determinations, such as whether the granting of access would endanger the individual or other persons so as to better understand how the time needed for these reviews relates to the overall time needed to provide the individual with access.

Comments regarding all of these proposed modifications must be submitted by **September 13, 2010.**