American Hospital Association

Legal Advisory

August 11, 2010

HITECH'S MODIFICATIONS TO HIPAA REQUIREMENTS: THE PROPOSED RULE

AT A GLANCE

The Issue:

The Department of Health and Human Services (HHS) in the July 14 *Federal Register* proposed certain modifications to the privacy, security and enforcement requirements of the *Health Insurance Portability and Accountability Act of 1996* (HIPAA), largely to implement changes necessitated by the *Health Information Technology for Economic and Clinical Health Act* (HITECH). The proposed revisions would:

- Limit or otherwise affect the use and disclosure of individuals' protected health information (PHI);
- Require business associates to comply with specific HIPAA privacy and security requirements and impose direct liability for their noncompliance with these regulatory standards; and
- Alter slightly HHS' complaints investigation procedures and offer some additional clarity about certain levels of HITECH-imposed culpability and the imposition of civil money penalties for HIPAA violations.

Comments on HHS' proposals are due by September 13.

Our Take:

The proposed revisions generally track HITECH's mandates, and will impose significant changes on hospitals' use and disclosure of PHI, necessitating changes to policies and procedures and amendments to the Notice of Privacy Practices. The revisions also will affect hospitals' business associate relationships, requiring the amendment of existing agreements and ways to ensure compliant provisions are include new agreements in the future.

While the majority of the HITECH-mandated changes already are statutorily effective (as of February 18, 2010), HHS recognizes the difficulties of complying before a final rule is issued. In addition, recognizing that some period beyond the final rule's effective date will be necessary, HHS intends to provide additional time beyond the effective date for compliance with most of the final rule's provisions. HHS also hopes to alleviate some burdens of changing ongoing existing business associate agreements with a grandfathering proposal. However, the enforcement rule modifications generally would be applicable at the time a final rule becomes effective.

What You Can Do:

- ✓ Share this advisory with your legal counsel, privacy and security officers, and other members of the HIPAA implementation team.
- ✓ Understand how the proposed revisions may impact your hospital's policy and procedures on the use and disclosure of PHI, any business associate relationships, and your organization's overall approach to HIPAA compliance.
- ✓ Use the release of this proposed rule as an early opportunity for advance planning to ensure your organization will be ready to comply with the revised provisions in the final rule within 180 days of the rule's effective date.
- ✓ Plan to participate in an AHA conference call on the proposed rule and provide feedback about the proposed changes.

Further Questions:

Please contact Lawrence Hughes, AHA assistant general counsel, at (202) 626-2346 or lhughes@aha.org.

AHA's Legal Advisories are produced whenever there are significant developments that affect the job you do in your community. A 44-page, in-depth examination of this issue follows.

August 11, 2010

HITECH'S MODIFICATIONS TO HIPAA REQUIREMENTS: THE PROPOSED RULE

TABLE OF CONTENTS

Background

The Department of Health and Human Services (HHS) in the July 14 *Federal Register* proposed certain modifications to the privacy, security and enforcement requirements of the *Health Insurance Portability and Accountability Act of 1996* (HIPAA), largely to implement changes necessitated by the *Health Information Technology for Economic and Clinical Health Act*(HITECH). The proposed revisions would:

- Limit or otherwise affect certain uses and disclosures of individuals' protected health information (PHI);
- Require business associates, expanded to a broader group of entities, to comply with specific HIPAA privacy and security requirements and impose direct liability for their noncompliance with these regulatory standards; and
- Alter slightly HHS' complaints investigation procedures and offer some additional clarity about certain levels of HITECH-imposed culpability and the imposition of civil money penalties for HIPAA violations.

Comments on HHS' proposals are due by September 13.

At Issue

Proposed Changes Affecting Use and Disclosure of PHI

Consistent with HITECH, HHS proposes a number of changes to the HIPAA privacy rules that affect the use and disclosure of PHI for marketing and fundraising, restrict the sale of PHI, obligate covered entities to honor an individual's request to restriction disclosure of PHI in certain circumstances, permit greater use and disclosure of PHI of decedents, allow disclose of students' immunization records, require updates to the Notice of Privacy Practices (NPP), and increase covered entities' flexibility in obtaining individual authorizations for use and disclosure of PHI for research. HHS also uses the proposed rule to request comments about the privacy rule's "minimum necessary" requirements.

Additional limits on marketing communications. HHS proposes to revise the definition of "marketing" in the privacy rule to make it consistent with HITECH's specific requirements. Under the privacy rule, covered entities generally must obtain a valid authorization to use or disclose an individual's PHI to market a product or service to that individual. The rule currently defines marketing as "making a communication about a product or service that encourages recipients of the communication to purchase or use the product or service," but it also

includes specific exceptions to the definition that would permit a covered entity to make, without an individual's authorization, certain health-related communications that otherwise qualify as marketing under that definition.

HITECH further restricts the health-related communications that would fall outside the definition of “marketing” and, thus, would not require that an individual’s authorization be obtained in order for the covered entity to make the communication. Under HITECH, a covered entity that receives, or has received, direct or indirect payment in exchange for making certain communications is required to obtain the individual's valid authorization prior to making the communication, or, if applicable, prior to its business associate making the communication on the covered entity’s behalf. Congress intended HITECH’s language to curtail a covered entity's ability to use the existing exceptions in the privacy rule’s marketing definition to send to individuals certain health-related product or service communications that were motivated more by commercial gain or another commercial purpose rather than for the purpose of the individual's health care.

To implement these additional HITECH restrictions, HHS proposes to now require a valid authorization when the covered entity receives financial remuneration in exchange for making a communication:

- About health-related products or services offered by a health care provider to individuals, including communications for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers or settings of care to the individual, unless certain notice and opt out conditions are met.

- For case management or care coordination, or contacting an individual with information about treatment alternatives, and related functions, to the extent these activities do not fall within the privacy rule’s current definition of treatment.

- Reminding about refills or otherwise about a drug or biologic that is currently being prescribed for the individual, unless any financial remuneration received is reasonably related to the cost of making the communication. HHS requests comment on the scope of this exception (*i.e.*, whether communications about drugs that are related to the drug currently being prescribed, such as generic alternatives or new formulations should fall within the exception,) as well as the types and amount of costs that should be allowed as reasonably related to the cost of making the communication.

- To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication.

In addition, HHS propose to eliminate the current regulation language that includes within the "marketing" definition "an arrangement between a covered entity and any other entity in which the covered entity discloses PHI to the other entity, in exchange for 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." This describes a "sale" of PHI under HITECH that now would be subject to particular new regulatory requirements described below.

Although in limiting permissible communications HITECH explicitly refers to "direct or indirect payment," HHS has substituted the term "financial remuneration" to avoid confusion since the privacy rule uses "payment" to mean payment for health care services and the rule's authorization requirements for marketing otherwise use the term "remuneration." HHS proposes to define "financial remuneration" to mean "direct or indirect payment from or on behalf of a third party whose product or service is being described." However, remuneration would not include any direct or indirect payment for the treatment of the individual. Additionally, only the receipt of financial remuneration in exchange for making a communication is relevant here.

The proposed rule would require authorization, for example, prior to a covered entity making a communication to patients about its acquisition of new state of the art medical equipment if the equipment manufacturer paid for the communication. In contrast, an authorization would not be required if a local breast cancer foundation funded a mailing about the availability of the covered entity's new state of the art mammography screening equipment, since the remuneration does not come by, or on behalf of, the entity whose product or service is being described (*i.e.*, the screening equipment manufacturer). Furthermore, no authorization would be required for a hospital to send 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 remuneration to the hospital from the third party was not in exchange for mailing the flyers.

The preamble clarifies that the revised definition of "marketing" does not impact a provider's face-to-face communications an individual about products or services or a covered entity's provision of promotional gifts of nominal value. These communications may continue to be made without obtaining an authorization or meeting the notice and opt out requirements. The preamble also clarifies that any communications to individuals promoting health in general, such as communications about the importance of maintaining a healthy diet or getting an annual physical, are still not considered marketing. General health promotion does not promote a specific product or service, and would not require individual authorization or compliance with the revised notice and opt out requirements. Similarly, communications about government and government-sponsored programs do not count as "marketing" because there is no commercial

component involved in communications about benefits available through public programs. Communications about government and government-sponsored programs also can be made without obtaining an authorization or meeting the notice and opt out requirements.

HITECH expressly provides that a communication to an individual that encourages the purchase or use of a health-related product or service where the covered entity receives payment from a third party in exchange for making the communication ***shall not be*** considered a "health care operation" under the privacy rule and, therefore, would constitute "marketing." However, as HHS explains, it is unclear precisely how Congress intended these provisions to apply to treatment communications between a health care provider and a patient, specifically whether Congress intended to restrict only subsidized communications about products and services that are less essential to an individual's health care (*i.e.*, those classified as health care operations communications) or all subsidized communications about products and services, including treatment communications. Given this ambiguity and to avoid preventing health care providers from communicating with an individual about health-related products or services that are necessary for the individual's treatment, HHS does not propose to require individual authorization where financial remuneration is received by the provider from a third party in exchange for sending to individuals "treatment" communications about health-related products or services.

HHS instead proposes to require the covered entity that intends to send written subsidized treatment communications to an individual to give notice, and to provide opportunity for the individual to opt out of receiving the communications. According to HHS, this proposal would ensure individuals are aware of the potential that he or she may receive, and get an early opportunity to opt out of, subsidized treatment communications from the provider. Essentially, the revised rule would permit a hospital to send written subsidized treatment communications without authorization **only if** the hospital:

- Includes a precise statement in the hospital's notice of privacy practices informing individuals that the hospital may send them treatment communications concerning treatment alternatives or other health-related products or services for which the hospital may receive financial remuneration from a third party in exchange for making the communication, and that individual has a right to opt out of receiving such communications.

- Provides with individual with the opportunity to exercise the choice to opt out.

- Discloses in the treatment communication itself that the hospital received remuneration and provides the individual with a clear and conspicuous opportunity to elect not to receive any further such communications.

As HHS states, the method used for the "opt out" may not cause the individual to incur an undue burden or more than a nominal cost. Therefore, HHS encourages covered entities to consider using a toll-free phone number, an e-mail address, or similar opt out mechanism that would provide individuals with a simple, quick, and inexpensive way to opt out of receiving future communications. On the other hand, HHS cautions that requiring individuals to write and send a letter to the covered entity asking not to receive future communications would constitute an undue burden on the individual and therefore would not satisfy the revised requirement.

HHS requests comment on how the opt out should apply to future subsidized treatment communications, whether specifically an "opt out" should, for example, prevent all future subsidized treatment communications by the provider or just those dealing with the particular product or service described in the specific communication. ***HHS also requests comment on the workability of requiring health care providers that intend to send subsidized treatment communications to individuals to provide an individual with the opportunity to opt out of receiving such communications prior to the individual receiving the first communication and what mechanisms could be put into place to implement such a requirement.***

The preamble cautions that the revised marketing provision would apply differently depending on whether a communication is for "treatment" or for "health care operations" and that clearly understanding of the difference between the two types of communications will be important for proper compliance. To promote a clearer understanding of the impact of revised proposal, the preamble offers the following particular principles for determining when health-related communications would require individual authorization if financial remuneration is involved:

- First, a health plan's communications concerning health-related products or services included in a plan of benefits or for case management or care coordination are ***never*** for "treatment" purposes, rather would always be "health care operations," and under the revised rule, would require individual authorization.

- Second, if made in a population-based fashion (*i.e.*, for health care operations), a health care provider's subsidized communications about health-related products or services for case management or care coordination or to recommend alternative treatments or settings of care would require individual authorization. But, if made to further the

treatment of a particular individual based on that individual's health care status or condition (*i.e.*, for treatment), would require the covered entity to give advance notice and to provide the individual with the opportunity to opt out.

Essentially, a provider who, for example, sends a pregnant patient a brochure recommending a specific birthing center suited to the patient's particular needs is recommending a setting of care specific to the individual's condition, which constitutes treatment of the individual. If the provider receives financial remuneration for mailing the brochure, the provider would under the revised regulation need:

- To have previously included in its notice of privacy practices a statement informing individuals that it may send subsidized treatment communications to them and that an individual has a right to opt out of such communications;
  and
- To disclose the fact of remuneration in the communication about the brochure and provide the individual with information on how to opt out of receiving future such communications.

In contrast, a health care provider who sends a blanket mailing to all patients with information about a new affiliated physical therapy practice would not be making a treatment communication. Rather, the provider would be making a communication for health care operations. If the provider receives financial remuneration for the communication, it would need under the revised regulation to get individuals' authorization to make the communication. Without authorization, the provider would be making an impermissible marketing communication.

Aware of the difficulty in making what may be in some cases close judgments and of potential unintended adverse consequences to a covered health care provider's ability to provide treatment to an individual, ***HHS requests comment on the proposed revision, including whether the revised rule should simply exempt treatment communications altogether from the authorization requirements even if they involve financial remuneration from a third party or, alternatively, whether it should require individual authorization for both treatment and health care operations communications made in exchange for financial remuneration.***

Limitations on the sale of PHI. To implement HITECH's limitations on the sale of PHI, HHS proposes to require a covered entity to obtain individual authorization for any disclosure of PHI if the covered entity receives direct or indirect remuneration from, or on behalf of, the recipient of the disclosed PHI. The proposal also would require that the authorization expressly state that the disclosure will result in remuneration to the covered entity. These requirements

also would apply to business associates as the statutory language of HITECH provides. HITECH specifically applies this limitation to any disclosures for remuneration occurring six months after the date the final implementing regulations are issued.

However, as enumerated in the statutory language of HITECH, the obligation to obtain an authorization would not extend to certain disclosures made in exchange for remuneration which are described below. HHS also would include an additional exception the Secretary "deems to be similarly necessary and appropriate," specifically exercising the general authority granted to the Secretary by HITECH to establish additional exceptions.

HHS' proposal would specifically exempt from the requirement to obtain individual authorization a covered entity's (or a business associate's) disclosures of PHI for:

- ***Public health activities*** as described in sec. 164.512(b) of the privacy rule, including disclosures of a limited data set for these activities.

- ***Research purposes*** as described in sec. 164.512(i) of the privacy rule (pertaining to IRB or privacy board waiver of authorization) and disclosures of a limited data set, as long as the remuneration received is a reasonable, cost-based fee to cover the cost to preparing and transmitting the information. ***HHS requests comment on the types of costs that should be permitted for this exception.***

- ***Treatment and payment.*** Though HITECH explicitly addressed only treatment, HHS includes in the proposed rule disclosures for payment purposes by referencing sec. 164.506(a) of the privacy rule, which establishes the standard for disclosures for treatment and payment purposes. HHS also proposes to exclude payment disclosures from the remuneration limitation to make clear that the exchange of PHI to obtain "payment" as the term is defined in sec. 164.501 of the rule is not a sale of PHI that would be subject to the individual authorization requirements.

- ***Sale, transfer, merger or consolidation*** of all or part of a covered entity with another covered entity, or an entity that following such activity will become a covered entity, ***and due diligence related to these activities***.

- ***Activities that the business associate undertakes on behalf of a covered entity*** as long as the only remuneration provided is from the covered entity to the business associate for the performance of a permissible business associate function. This proposed exception also would exempt from the authorization requirement the business associate's disclosure of PHI to a third party on behalf of the covered entity as long as any remuneration received by the business associate was payment from

the covered entity for the permissible business associate activities performed pursuant to a compliant business associate contract.

- The ***individuals who request access to their own PHI*** or an accounting of disclosures. However, the preamble specifically cautions that this exception would **not** permit a covered entity to require that an individual pay a fee for access to their own PHI or for the accounting that is not otherwise permitted by the privacy rule

- ***Required by law*** as permitted under sec. 164.512(a) of the privacy rule.

- ***Any other purpose permitted by and in accordance with the applicable requirements of the privacy rule***, as long as the only remuneration received by the covered entity is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or is a fee otherwise expressly permitted by other law, include fees permitted by any applicable state laws.

HHS invites comment on the proposed exceptions to the authorization requirement and whether additional exceptions should be included in the final regulation. HHS also indicates a specific interest in comments on the inclusion of the required by law and the more general exception for purposes permitted by the privacy rule described above.

HHS also requests comment on its decision not to include specific language in the revised regulation that parallels HITECH's precise reference that the authorization for the sale of PHI specify that PHI disclosed by the covered entity for remuneration can be further exchanged for remuneration by the receiving entity and its comment that a covered entity or business associate that receives PHI in exchange for remunerations would need to obtain another authorization before redisclosing that PHI in exchange for further remuneration. HHS believes the intent of the reference in HITECH was to ensure that the authorization include a statement about whether the covered entity will received remuneration for the disclosure subject to the authorization. Otherwise, HHS states, the individual would not be put on notice that the disclosure involves remuneration and thus, would not be making an informed decision as to whether to sign the authorization. Accordingly, HHS' proposes instead to require that the authorization include a separate specific statement that the covered entity is receiving direct or indirect remuneration in exchange for the PHI. As the preamble notes, there is no need to include a reference to HITECH's precise language because, if a covered entity (or its business associate) discloses PHI to another covered entity or business associate for remuneration in compliance with the revised authorization requirements, the recipient of the PHI could not redisclose that PHI in exchange for remuneration unless it also obtains a valid authorization for the redisclosure.

Finally, HITECH specifically calls for the Secretary to evaluate the impact on research or public health activities, including those conducted by or for the use of the Food and Drug Administration (FDA), of further restricting the exception for public health disclosures to ensure that the price charged for the data reflects *only* preparation and transmittal costs for the data. Further, HITECH states the Secretary may impose the additional regulatory restrictions if the Secretary finds that additional restriction will not impede these activities. ***While not proposing at this time to include that restriction on public health disclosures, HHS requests comment on the issue to assist in evaluating the potential impact of imposing such a limit on public health disclosures.***

Additional limits on the use and disclosure of PHI for fundraising. HHS also proposes a number of changes to apply HITECH's additional limitations to the privacy rule's fundraising provisions. The rule currently permits a covered entity, without an individual's authorization, to use an individual's demographic information or the dates an individual received health care services or to disclose that information to a business associate or an institutionally related foundation for the covered entity's own fundraising purposes.

First, HHS proposes to require the covered entity to provide, with each fundraising communication sent to an individual, a clear and conspicuous opportunity for the individual to actually elect not to receive further fundraising communications. This change would strengthen the current rule's "opt out" provisions which state that a covered entity must include in any fundraising materials it sends only a description of how the individual may opt out of receiving future fundraising communications.

Second, HHS proposes to require that the method a covered entity uses for an individual to opt out "may not cause the individual to incur an undue burden or more than nominal cost" in order to be compliance with the revised requirement. In the preamble, HHS encourages the use of a toll-free phone number, an e-mail address, or similar mechanism that would provide a simple, quick, and inexpensive way to opt out of receiving future communications. The preamble cautions that HHS would **NOT** consider requiring individuals to write and send a letter to the covered entity as an appropriate means of satisfying the requirement.

Additionally, under HHS' proposal, a covered entity ***may not*** send fundraising communications to an individual who has elected not to receive them. This proposed language is stronger than the current regulatory provision which requires "reasonable efforts" to ensure that no further fundraising communications are sent. HHS intends this change to make clear its expectation that covered entities abide by an individual's decision not to receive fundraising communications, as well as to ensure that the "opt out" operates more like a revocation of authorization which, according to HHS, is consistent with the statutory language and legislative history of the relevant HITECH provision.

Finally, the proposed rule would provide that a covered entity may not condition treatment or payment on an individual's choice about receiving fundraising communications. As the preamble indicates, this modification also is intended to implement HITECH's requirement that an individual's election equate to a revocation of authorization under the privacy rule. According to HHS, HITECH's legislative history indicates that congressional intent is that "the protections that apply to an individual who has revoked an authorization under the privacy rule similarly apply to an individual who has opted out of fundraising communications, 'including the right not to be denied treatment as a result of making that choice'."

While a covered entity that intends to contact individuals to raise funds would still be required to include a statement to that effect in its notice of privacy practices because HHS' proposal retains that provision from the current rule, HHS proposes a slight edit to the required statement: the covered entity also must inform individuals explicitly that they have a right to opt out of receiving fundraising communications.

HHS requests comment about how the opt out should precisely apply to fundraising communications, including whether it should apply to all future fundraising communications or be structured to apply only to the particular fundraising campaign described in the specific communication. In addition, HHS requests comment on what method, short of signing an authorization, the rule should permit for an individual who previously opted out to use to put his or her name back on an institution's fundraising list.

Finally, HHS solicits comment on the rule's current limits on the information (i.e., demographic information and dates of service) a covered entity may use or disclose for fundraising purposes. In the preamble discussion, HHS asks specifically whether the rule should permit additional categories of PHI to be used or disclosed for fundraising, (*e.g.*, the department of service where care was received or outcomes information) and what those categories should be. HHS also asks whether and how, if the rule permits the use and disclosure of additional information for fundraising absent an individual's authorization, it should require covered entities to provide individuals with an opportunity to opt out of receiving any fundraising communications before making the first solicitation as well as the opportunity to opt out with every subsequent communication.

<u>Enhanced right of individuals to request restriction of certain uses and disclosures</u>. HHS proposes to add a new section to the privacy rule that requires a covered entity to agree to an individual's request to restrict disclosures of the individual's PHI to a health plan if:

- The PHI pertains solely to a health care item or service for which the individual has paid the provider in full, or someone else other than a health plan has made a payment in full on behalf of the individual;

- The disclosure is for payment or health care operations; and

- The disclosure is not otherwise required by law.

HITECH's statutory requirement overrides the current rule's provision that establishes a general rule that the covered entity is NOT required to agree to requests for restrictions, and accordingly, requires HHS to modify the current provision.

As the preamble states, the mandatory restriction on disclosures also would cover disclosure to a business associate of the health plan because "under the Privacy Rule, a covered entity may make a disclosure to a business associate of another covered entity only where the disclosure would be permitted directly to the other covered entity."

The preamble makes two additional points about the proposed change: first, the term "required by law" is specifically defined in the current HIPAA privacy regulation at Sec. 164.103, and HHS does not alter its meaning in the proposed rule. ***HHS expresses specific interest in receiving comment on examples of the types of disclosures that may fall under this provision and that would permit the disclosure of PHI to the health plan, despite the individual's request for a restriction.***

Second, "payment in full" is not limited solely to payment made by the individual making the request for the restriction. There are many situations in which family members or other persons may pay for the individual's treatment. Thus, this proposed change would provide that as long as the covered entity is paid in full for the services by the individual or "another person on the individual's behalf other than the health plan," the covered entity would be required to honor the restriction.

The preamble also cautions that an individual should not expect that this payment will count towards the individual's out of pocket threshold with respect to his or her health plan benefits when requesting a disclosure restriction and paying out of pocket for the treatment or service. The very nature of this provision is to restrict information from flowing to the health plan; and consequently, the health plan will be unaware of any payment for treatment or services for which the individual has requested a restriction.

HHS specifically requests comment on how this provision will function with respect to HMOs. Typically, under an HMO contracts, the provider receives a fixed payment from an HMO based on the number of patients seen and not on

the treatment or service provided; and an individual patient pays the provider a flat co-payment for every visit regardless of the treatment or service received. Therefore, according to HHS' understanding, most current HMO contracts with providers do not permit an individual to pay "in full" for the treatment or service received which may necessitate that individuals who belong to an HMO use an out-of-network provider if they wish to ensure that certain PHI is not disclosed to the HMO.

Finally, the preamble notes that HHS does not believe that the statutory intent of the mandatory restriction is to permit individuals to avoid payment to providers for the health care services they have received. Therefore, if an individual's out of pocket payment for a health care item or service is not honored (for example, the individual's check bounces), the covered entity then may submit information to the health plan for payment because the individual has not fulfilled the requirements necessary to obtain a restriction. However, HHS expects covered entities to make some attempt to resolve the payment issue with the individual prior to sending PHI to the health plan, such as notifying the individual that his or her payment did not go through and giving the individual an opportunity to submit payment. ***HHS expresses interest in receiving comment on the extent to which covered entities must make reasonable efforts to secure payment prior to sending information to the health plan for payment.***

The preamble provides insight about how the proposed changes would affect a covered entity's termination of a restriction since the privacy rule's current termination provision is not applicable to this mandatory restriction. An individual who previously requested a restriction on the disclosure to a health plan of PHI about a particular health care service, for example, again visits the provider for follow-up treatment. This time the individual asks the provider to bill the health plan for the follow-up visit, and does not request a restriction nor pay out of pocket for the follow-up treatment. While there is no restriction in effect with respect to the follow-up treatment, the provider may need to submit information about the original treatment to the health plan so that it can determine the medical appropriateness or medical necessity of the follow-up care provided to the individual. HHS indicates that, at this time, the lack of a restriction with respect to the follow-up treatment would extend to any PHI necessary for payment for the follow-up treatment, even if the information was subject to a prior restriction. HHS encourages covered entities to have an open dialogue with individuals in this situation to ensure that they are aware that PHI may be disclosed to the health plan unless they request an additional restriction and pay out of pocket for the follow-up care. ***HHS also is interested in receiving comments about this issue.***

In HHS' view, HITECH provides the individual with the right to determine for which health care items or services the individual wishes to pay out of pocket and, thereby, restrict disclosures of relevant PHI. As a result, HHS does not believe a covered entity could require individuals who wish to restrict disclosures

about only certain health care items or services to a health plan to pay out of pocket for all services provided to take advantage of the right to restrict disclosure of information about the particular health care item or service for which the restriction is requested. For example, an individual who regularly visits the same provider for the treatment of both asthma and diabetes must be able to request, and have the provider honor, a restriction only on the disclosure of diabetes-related treatment to the health plan as long as the individual pays out of pocket for this care. The provider cannot require that the individual apply the restriction to all care given by the provider and, as a result, cannot require the individual to pay out of pocket for both the diabetes and asthma-related care in order to have the restriction on the diabetes care honored. Therefore, HHS encourages covered entities to work with individuals who wish to restrict certain information from disclosure to determine the best method for ensuring that the appropriate information is restricted.

HHS requests comment on the types of interactions between individuals and covered entities that would make requesting or implementing a restriction more difficult. HHS offers the specific example of a patient who receives treatment that the patient pays for out of pocket and requests the provider not disclose that information to the health plan, but also is prescribed a medication about which the patient also wishes to restrict disclosure to the health plan. Where the provider electronically sends the prescription to the pharmacy to be filled so that it will be ready for pick up when the patient arrives, the pharmacy already may have sent the information to the health plan before the patient arrives at the pharmacy. This would not give the patient an opportunity to request a restriction at the pharmacy. And, while the provider can always provide the individual with a paper prescription, this might not be practical in every case, especially as covered entities begin to replace paper-based systems with electronic systems. Therefore, ***HHS asks specifically for suggestions of methods through which a provider, using an automated electronic prescribing tool, could alert the pharmacy that the individual may wish to request a restriction on disclosure of prescription information.***

Additionally, HHS requests comment on the obligation of covered health care providers that know of a restriction to inform other downstream health care providers of the restriction. In HHS' precise example, a provider has been treating an individual for an infection for several months and the individual has requested restriction of any PHI relating to the treatment of the infection. The individual then requests that the provider send a copy of the medical record to another health care provider for treatment. HHS ask precisely what, if any, obligation should the original provider have to notify any recipient provider that a restriction applies to much of the PHI in the transferred medical record? Specifically, should a restriction placed upon certain PHI continue to apply to the information as it moves downstream, or should the restriction no longer apply until the individual visits the new provider for treatment or services, requests a restriction, and pays the new provider out of pocket for the treatment or services?

To what extent are technologies that would facilitate notification among providers of restrictions on disclosures currently available and in use? Are there any limitations in the technology that would require additional manual or other procedures to provide notification of the restriction?

Enhanced individual right of access to PHI in an electronic health record. HHS proposes to require that if individuals request access to their PHI and a covered entity maintains the PHI electronically in one or more designated record sets, the covered entity must provide the individual with access to the information:

- In the electronic form and format requested by the individual, if that is readily producible;
  or
- In a readable electronic form and format mutually agreed to by the covered entity and the individual, if the requested electronic form and format is not readily producible.

HHS' proposal is intended to implement HITECH's requirement to provide individuals with electronic access to their PHI when covered entities use or maintain an "electronic health record." HITECH also obligates a covered entity to transmit an electronic copy of the PHI directly to the individual's designee, provided that the patient's choice to direct the transmittal is clear, conspicuous, and specific. Additionally, HITECH limits any fee imposed by the covered entity for providing such an electronic copy, providing that the fee must not be greater than the entity's labor costs in responding to the request for the copy.

While by its specific terms, the HITECH requirement applies only to PHI in electronic health records, HHS suggests that such a limited incorporation of the HITECH requirement into the privacy rule could result in a complex set of disparate requirements for access to PHI in electronic health records systems compared to other types of electronic records systems. As a result, HHS proposes to use its general statutory authority under HIPAA to apply the right of access more uniformly to ***all PHI maintained electronically*** in one or more designated record sets, ***regardless whether the designated record set is maintained in an electronic health record***.

As the preamble notes, the individual's right of access to an electronic copy of PHI under the regulation is limited by whether the form or format requested is readily producible. However, the proposed revision would require some type of electronic copy of the PHI, upon the individual's request. Not wanting to bind covered entities to standards that may not yet be technologically mature, HHS accordingly would permit covered entities to make some agreement with the individual about an alternative means of providing a readable electronic copy, to the extent the requested means cannot be readily produced. For example, where the only readily producible version of the PHI is a portable document format (PDF), the proposed rule would require the covered entity to provide the

individual with a PDF copy if the covered entity and the individual agree, despite the individual's initial request that the covered entity provide electronic access via a secure Web-based portal. The preamble nevertheless make clear that "while there may be circumstances where a covered entity determines that it can comply with the Privacy Rule's right of access by providing individuals with limited access rights to their electronic health record, such as through a secure Web-based portal, nothing under the current rule or the proposed revision would require a covered entity to do so where the covered entity determines it is not reasonable or appropriate."

As the preamble points out, the option of arriving at an alternative agreement that satisfies both parties is already part of the current requirement to provide access. As a result, HHS does not believe that the extension of the requirement to electronic access would present implementation difficulties. HHS nevertheless expects that covered entities will ensure that reasonable safeguards are in place to protect the information when it provides an electronic copy to an individual through a Web-based portal, e-mail, on portable electronic media, or other means. ***HHS presumes that covered entities have the capability of providing security for an electronic copy sent through a Web-based portal, via e-mail, on portable electronic media, or other manner, but invites comments on that presumption.***

HHS also proposes to expressly provide that, if "clearly, conspicuously, and specifically" requested by an individual, a covered entity must transmit a copy of PHI directly to another person designated by the individual. To ensure that the individual's "choice [be] clear, conspicuous, and specific," HHS proposes to require that the individual's request be "in writing, signed by the individual, and [that it] clearly identify the designated person and where to send the copy." As the privacy rule currently allows, electronic documents qualify as written documents for purposes of meeting this requirement, and electronic signatures satisfy any signature requirements, to the extent an electronic signature is valid under applicable laws. Accordingly, under the proposed revision, a covered entity could employ an electronic process for receiving an individual's request to transmit a copy of PHI to his or her designee. However, regardless of whether the process is electronic or paper-based, a covered entity also must, as the current rule already requires, implement reasonable policies and procedures to verify the identity of any person who requests PHI, as well as implement reasonable safeguards to protect the information that is transmitted.

HHS also identifies separately in the proposed regulatory text that the "labor" for copying PHI, whether in paper or electronic form, is one factor that may be included in a reasonable cost-based fee that the rule permits covered entities to impose. While not specifying within the regulatory text detailed considerations for this factor, HHS makes clear that all prior interpretations of "labor" with respect to paper copies – more precisely, that the labor cost of copying may ***not*** include the costs associated with searching for and retrieving the requested

information – will continue in force under the revised rule. Accordingly, a reasonable cost-based fee for electronic copies includes costs attributable to the labor involved to review the access request and to produce the electronic copy (expect to be negligible). However, HHS would not consider a reasonable cost-based fee to include a standard "retrieval fee" that does not reflect the actual costs associated with retrieval or that reflects charges that are unrelated to the individual's request (*e.g.*, the additional labor resulting from technical problems or a workforce member's lack of adequate training). ***HHS invites comment on this issue, specifically about what types of activities related to managing electronic access requests should be compensable aspects of "labor."***

The HHS' proposal also provides separately for the inclusion of the cost of electronic media (*i.e.*, physical media such as a compact disc (CD) or universal serial bus (USB) flash drive), if the individual requests that the electronic copy be provided on portable media. According to HHS, HITECH permits only the inclusion of labor costs in the charge for electronic copies, and by implication excludes charging for the supplies that are used to create an electronic copy, such as the hardware (computers, scanners, etc.) or software that is used to generate the electronic copy. An electronic copy, in contrast to a hard copy which generally exists on paper, is independent of media, and can be transmitted securely via multiple methods (*e.g.*, e-mail, a secure Web-based portal, or an individual's own electronic media) without accruing any ancillary supply costs. Of course, HITECH's limitation is in contrast to a covered entity's ability to charge for supplies for hard copies of PHI (*e.g.*, the cost of paper, the prorated cost of toner and wear and tear on the printer). See 65 FR 82462, 82735, Dec. 28, 2000 (indicating that a covered entity was free to recoup all of their reasonable costs for copying in a response to a request for clarification on "capital cost for copying" and other supply costs).

Under HHS' proposal, a covered entity may charge a reasonable and cost-based fee for any electronic media it provides, as requested or agreed to by an individual who does not supply his or her own. For example, a covered entity could charge a reasonable cost-based fee for the encrypted USB flash drive where an individual has requested that the copy be placed on electronic media (such as a recordable CD) but failed to bring his or her own. In contrast, if an individual has brought his or her own electronic media (such as a recordable CD) and the covered entity's systems are readily able to place the electronic copy on supplied media, the covered entity would not be allowed to require the individual to purchase an encrypted USB flash drive instead. In addition, if an individual requests that an electronic copy be sent via unencrypted e-mail, the covered entity should advise the individual of the risks associated with unencrypted e-mail, but would not be allowed to require the individual to instead purchase a USB flash drive.

As HHS notes, this interpretation of HITECH also would permit a covered entity to charge for postage if an individual requests that the covered entity transmit

portable media containing an electronic copy through the mail or via courier (*e.g.*, if the individual requests that the covered entity save PHI to a CD and then mail the CD to a designee).

Finally, while HITECH did not change the timeliness requirements for provision of access, HHS is requesting comment on this aspect of the right to access. Under the current requirements in the rule, a request for access must be approved or denied, and if approved, access or a copy of the information provided, within 30 days of the request. In cases where the records requested are only accessible from an off-site location, the covered entity has an additional 30 days to respond to the request. In extenuating circumstances where access cannot be provided within these timeframes, the covered entity may have a one-time 30-day extension if the individual is notified of the need for the extension within the original timeframes.

As HHS notes, the advancement of electronic health records systems has created rising expectation for, and increasing capacity to provide, almost instantaneous electronic access to the PHI stored in personal health records or accessed through similar electronic means. However, HHS, because it does not propose to limit the right to electronic access to certified electronic health records, is sensitive that the variety of electronic systems that proposed access requirement would therefore apply to probably are not all capable of complying with a timeliness standard based on the precise capabilities of an electronic health records system. Therefore, HHS assumes that a single timeliness standard that would address a variety of electronic systems, rather than having a multitude of standards based on system capacity, would be the preferred approach to avoid workability issues for covered entities. HHS is interested in specific comments on an appropriate, common timeliness standard, including comments on:

- Aspects of existing systems that would create efficiencies in processing of requests for electronic information, as well as aspects of systems that would not provide much change from the time required for processing a paper record.

- 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.

- Whether, contrary to HHS' assumption, the preferred approach to timeliness should be a variety of standards based on the type of electronic designated record; and if so, how should such an approach be operationalized, including how to identify and characterize the various electronic record sets (*e.g.*, personal health records, electronic health records, others) to which a specific standard would apply; what functionality within these electronic systems would drive the need for more

or less time to provide the individual with electronic access; what timeliness standards would be appropriate for the different systems; what timeliness standard(s) would be required of entities that have PHI spread across hybrid systems that have different functionalities; and what would be the impact and the challenges of having multiple timeliness standards for access.

- The time needed to review access requests and make necessary determinations, such as whether granting access would endanger the individual or other persons, to help HHS understand how review time relates to the overall time needed to provide the individual with access to the information.

- Whether the provision which allows a covered entity an additional 30 days to provide access to the individual if the PHI is maintained off-site should be eliminated altogether for both paper and electronic records, or at least for PHI maintained or archived electronically because the physical location of electronic data storage may not relevant to its accessibility.

Finally, as the preamble cautions, even under a single standard, nothing would prevent electronic health record systems from being developed through HITECH's standards and certification process with the technological capabilities to exceed the privacy rule's timeliness requirements for providing access.

Easing restrictions on use and disclosure of decedents' PHI. HHS proposes that the privacy rule limitations on the use and disclosure of PHI would apply to a deceased individual's PHI only for a period of 50 years following the date of the decedent's death. Currently, to the extent a decedent's information is maintained by a covered entity, it is perpetually subject to the privacy rule limitations on use and disclosure. HHS intends this proposed change to respond specifically to covered entities' expressed concerns about the difficulty of locating, especially after closure of an estate, a decedent's personal representative to authorize the use or disclosure of the decedent's PHI as well as to the frustrations related by archivists, biographers and historians about the lack of access to historically valuable records held by covered entities, even when few individuals remain who may have concerns about the privacy of the information. To complement this proposed change, the definition of "protected health information" in the rule would be modified to clearly exclude individually identifiable health information of a person who has been deceased for more than 50 years.

HHS suggests that 50 years is an appropriate time span, because it covers approximately the span of two generations and as a result, will protect the privacy interests of most, if not all, living relatives, or other affected individuals. It also reflects the difficulty with the passage of time of obtaining authorizations from a decedent's personal representative. ***Nevertheless, HHS requests comment on the appropriateness of the 50-year time period.***

In addition, the proposed rule would permit covered entities to disclose a decedent's information to family members and others who were involved in the decedent's care or payment for care prior to death, unless doing so is inconsistent with any prior expressed preference of the decedent that is known to the covered entity. This proposed change is intended to respond to concerns expressed by family members, relatives, and others, many of whom may have had access to the health information of the deceased individual prior to death, about difficulties in obtaining access to such information after death, because they do not qualify as a "personal representative" of the decedent. Under the current rule, the "personal representative" is the executor, administrator, or other person authorized by applicable state laws to act on behalf of the decedent or the decedent's estate. As the preamble discussion states, this type of disclosure would be permitted, but not required. ***HHS requests comment on any unintended consequences that making this disclosure a permissive provision might cause***.

As the preamble states, the proposed modifications would have no impact on a covered entity's disclosures of decedents' PHI for law enforcement purposes (Sec. 164.512(f)(4)); to coroners or medical examiners and funeral directors (Sec. 164.512(g)); for research that is solely on the PHI of decedents (Sec. 164.512(i)(1)(iii)); and for organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation (Sec. 164.512(h)). These disclosures are governed specifically by other privacy rule provisions.

Additionally, the proposed revision does not affect the authority of a decedent's personal representative who may continue to request access to or an accounting of a decedent's PHI, and to authorize uses and disclosures of the decedent's PHI that are not otherwise permitted or required by the privacy rule.

Permitted disclosure of immunizations records to schools. HHS proposes to add a new provision that would permit covered entities to disclose proof of students' immunizations to schools in states that have school entry or similar laws. HHS' proposal still would require a covered entity to obtain agreement, which may be oral, from a parent, guardian or other person acting *in loco parentis*, or directly from the student who is either an adult or emancipated minor. However, a written compliant authorization would no longer be required for the disclosure. ***HHS requests comments on this proposal***, including specifically:

- Whether a provider should document any oral agreement to help avoid such problems as miscommunication and the later objection by a parent, or whether a written documentation requirement would be, on balance, overly cumbersome.

- Whether the rule should require that disclosures go to a particular school official and, if so, who.

- Whether a precise definition of "school" should included in the regulation itself and whether it should include schools not subject to school entry laws but that may also require proof of immunization that would warrant their inclusion in this disclosure category because these schools also have experienced problems accessing students' immunization records.

The preamble notes that once a student's immunization records are obtained and maintained by an educational institution or agency to which the *Family Educational Rights and Privacy Act* (FERPA) applies, they are protected by FERPA, not the HIPAA privacy rule. HHS specifically encourages organizations to consult the Joint HHS/ED Guidance on the Application of FERPA and HIPAA to Student Health Records at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hipaaferpajointguide.pdf for more information.

Inclusion of additional information in the Notice of Privacy Practices. HHS proposes to require that the Notice of Privacy Practices (NPP) include specific separate statements that actually ***describe*** the uses and disclosures of PHI that require an authorization: psychotherapy notes (sec. 164.508(a)(2)); marketing (sec. 164.508(a)(3)) and sale of PHI (sec. 164.508 (a)(4)). The NPP also must state specifically that "other uses and disclosures not described in the notice will be made only with the individual's written authorization." The rule currently requires that the NPP contain the statement that "any uses and disclosures other than those permitted by the Privacy Rule" will be made only with the written authorization of the individual, and that the individual has the right to revoke an authorization as provided by section 164.508(b)(5) of the rule.

The proposed revision, as preamble states, would ensure that covered entities notify individuals that most disclosures of PHI for which the covered entity receives remuneration would require individual authorization. It also would require that covered entities provide the specific notice about psychotherapy notes and marketing so that individuals will be made aware of all situations in which authorization is required. HHS is concerned that omission of such a specific statement may be somewhat misleading or confusing, because the NPP would otherwise state that the covered entity may use or disclose PHI without authorization for treatment, payment, and health care operations and some individuals might assume that psychotherapy notes and marketing would be covered by these permissions.

In addition, HHS proposes modification to certain required statements what must be included separately in the NPP that let individuals know that the covered entity intends to contact them to provide certain health related communications or to solicit for fundraising. These proposed modifications would align the

requirements for the NPP with the proposed additional use and disclosure limitations discussed in previous sections of this Advisory. Precisely, a covered health care provider that intends to:

- Send communications about ***treatment alternatives or other health-related products or services where the provider receives financial remuneration*** in exchange for making the communication must inform individuals of this intention in advance in the NPP, as well as let them know of the opportunity to opt out of receiving such communications.

- Contact the individual to ***raise funds*** for the entity must not only inform individuals in the NPP of this intention and also let individuals know they have the right to opt out of receiving such communications.

HHS also proposes to require an edit to the statement that notifies individuals of the right to request restrictions on disclosures of PHI because the current required statement will no longer be accurate when the HITECH modifications to enhance the right of individuals to request restriction of certain disclosures discussed previously are effective. The statement that the covered entity is not required to agree to a request for restriction would now include an exception in the case of a use or disclosure of PHI to a health plan that meets the precise requirements of this proposed new regulatory provision.

The preamble underscores that the proposed modifications to the NPP described above represent material changes; and accordingly, covered entities are required to promptly revise and distribute the NPP as outlined in existing sec. 164.520(c) of the privacy rule. The current requirement for a health care provider with a direct treatment relationship with an individual states that the provider must make the revised NPP available upon request ***on or after the effective date of the revision*** and must meet particular requirements about the availability of the NPP at the site where care is deliver and posting in a clear and prominent location. ***HHS suggests that these current revision and distribution requirements will not be overly burdensome on health care providers and proposes no changes to them. HHS nevertheless asks for comments.***

In contrast, HHS suggests that revising and redistributing the NPP may be costly for health plans which, under the existing requirement must provide notice to individuals covered by the plan within 60 days of any material revision to the NPP. ***HHS outlines in the preamble at page 40898 a number of specific options to ensure that the process is not unduly burdensome for health plans and requests comments about them.***

Finally, ***HHS requests comment on whether the Privacy Rule should require a specific statement regarding the new legal duty of covered entities and business associates to comply with the requirements for notification to affected individuals, the media, and the Secretary following a breach of***

unsecured PHI, and what particular aspects of this new obligation would be important for individuals to be notified about in the NPP.

Permitting certain compound authorizations for research. HHS proposes to relax the privacy rule's current general prohibition on "compound authorizations," (*i.e.*, where an authorization for the use and disclosure of PHI is combined with any other legal permission). The current requirement prohibits combining an authorization that conditions treatment, payment, enrollment in a health plan, or eligibility for benefits with an authorization for another purpose for which treatment, payment, enrollment, or eligibility may not be conditioned. The current limitation on compound authorization is intended to help ensure that individuals understand that they can receive treatment or other benefits or services by agreeing to the conditioned authorization while simultaneously declining to participate in the activity described in the unconditioned authorization.

Generally, the privacy rule does not permit a covered entity to condition treatment, payment, enrollment in a health plan or eligibility for benefits on an individual authorizing the use or disclose of their PHI. However, in limited situations such as for a clinical trial, the current rule permits a covered entity to condition the provision of research-related treatment on obtaining the individual's authorization to use and disclosure PHI: permitting the use and disclosure of PHI is part of the decision to receive care through a clinical trial.

The rule's current general prohibition on "compound authorizations," carves out an exception that permits combining an authorization for a research study with any other written permission for the same study, including another authorization or consent to participate in the research. But the rule's current limitations directly impact clinical trials that are associated with a corollary research activity, such as when PHI is used or disclosed to create or to contribute to a central research database or repository. For example, the covered entity is prevented from obtaining a single authorization for the use or disclosure of PHI for a research study that includes both treatment as part of a clinical trial and tissue banking of specimens (and associated PHI) collection. A research-related treatment authorization generally is conditioned while a tissue and data banking authorization generally is not conditioned. Under the current rule, the covered entity would still need to obtain separate authorizations from research participants for a clinical trial that also collects specimens with associated PHI for a central repository.

As HHS explains, the current rule provides an option to seek Institutional Review Board (IRB) or Privacy Board waiver of the authorization requirement. However, an IRB or Privacy Board may be less likely to approve a request for a waiver of authorization for a foreseeable use or disclosure of PHI to create and maintain or contribute to a central tissue or information repository if the covered entity is planning to seek informed consent from the individual for this purpose.

Accordingly, the rule's current waiver provisions generally do not resolve concerns expressed by the research community.

HHS' proposal would allow a covered entity to combine conditioned and unconditioned authorizations for research, if the authorization clearly:

- Differentiates between the conditioned and unconditioned research components;
  and
- Allows the individual the option to opt in to the unconditioned research activities.

These proposed revisions would allow covered entities to combine authorizations for many scenarios that often occur in research studies, including, for example, combining an authorization permitting the use and disclosure of PHI associated with a specimen collection for a central repository with an authorization permitting use and disclosure of PHI for clinical research that conditions research-related treatment on the execution of a HIPAA authorization.

HHS suggests that allowing the combination of research authorizations would streamline the process of obtaining authorizations and would make the documentation responsibilities of covered entities more manageable. This is critically important for clinical research trials that may have thousands of participants and for which documenting and storing twice as many authorizations is a current concern.

The combination authorization also would create a simpler and, therefore, more meaningful authorization for research participants. HHS reports that recruitment into clinical trials has been hampered, in part, because the multiplicity of forms for research studies dissuades individuals from participating and that redundant information provided by two authorization forms (*i.e.*, one for the clinical study and another for related research) diverts an individual's attention from other content that describes how and why PHI may be used.

HHS cautions that the proposed modifications would not alter the core elements or required statements integral to a valid HIPAA authorization, but would give covered entities some flexibility with respect to how they met the authorization requirements. For example, covered entities could facilitate an individual's understanding of a compound authorization by describing the unconditioned research activity on a separate page of a compound authorization. They also could cross-reference relevant sections of a compound authorization to minimize the potential for redundant language. In addition, a covered entity could use a separate check-box for the unconditioned research activity to signify whether an individual has opted-in to the unconditioned research activity, while maintaining one signature line for the authorization. Alternatively, a covered entity could choose to provide a distinct signature line for the unconditioned authorization to

signal that the individual is authorizing optional research that will not affect research-related treatment. ***HHS requests comment on additional methods that would clearly differentiate for an individual the conditioned and unconditioned research activities on the compound authorization.***

Authorizing use and disclosure for future research. Although it does not currently propose any specific modifications to the privacy rule, HHS also is considering whether to modify its current interpretation that the rule requires that a valid authorization for the use or disclosure of PHI for research be research-study specific. As HHS explains, the current interpretation in part was intended to respond to concerns that patients may lack necessary information in the authorization to make an informed decision about the future research, due to a lack of information about the future research at the time the authorization is obtained. An authorization compliant with the current rule provision is required to include a description of each purpose for the requested use or disclosure.

HHS explains that this approach was intended to facilitate patients' informed decisions about future research. HHS also notes that a covered entity would not always need to re-contact an individual for future research, but instead could obtain a waiver of authorization from an IRB or Privacy Board, or use or disclose only a limited data set under a compliant data use agreement. As HHS explains, the agency believes that IRBs in some cases may approve an informed consent document for a clinical trial that also asks research participants to permit future research on their identifiable information or specimens obtained during the course of the trial, or may review an informed consent for a prior clinical trial to determine whether a subsequent research use is encompassed within the original consent. Therefore, covered entity would not necessarily have to bear the burdens associated with re-contacting individuals to obtain another authorization for the additional research. HHS notes, however, that there have been a number of concerns express about the impact of these requirements on research and that, as a result, HHS is considering whether to modify its interpretation that a research authorization be study-specific.

HHS seeks comment on the issues related to authorizations for future research, anticipating that it will address, if appropriate, the issue at the time the final rule is issued. In particular, HHS is interested in comment about the impact on the research process and patients' understanding of authorizations, including whether the privacy rule should:

- Permit an authorization for future research if the purposes of the research are adequately described in the authorization in a way that it would be reasonable for the individual to expect that his or her PHI could be used or disclosed for the research.

- Permit an authorization for future research only if the description of the future research included certain elements or statements specified in regulation, and if so, what these elements or statements should be.

- Establish as a general rule that an authorization for future research is permitted when the purposes of the research are adequately described in the authorization in a way that it would be reasonable for the individual to expect that his or her PHI could be used or disclosed for the research, but require that the authorization include certain disclosure statements in cases where the research encompasses certain types of sensitive research activities, such as genetic analyses or mental health research, that may alter an individual's willingness to participate in the research.

HHS states that any modification in this area would not alter an individual's right to revoke the authorization for future research at any time and the authorization would be required to include a description of how the individual may revoke the authorization. ***HHS requests comment on how a revocation would operate with respect to future downstream research studies.***

Solicitation of comments for required guidance on minimum necessary uses and disclosures. HHS also uses the proposed rule to solicit comments to inform its development of guidance on minimum necessary use and disclosure of PHI that HITECH mandates HHS develop. Under HITECH, a covered entity is in compliance with HIPAA's minimum necessary requirement ***only if*** the covered entity limits its use and disclosure of PHI, to the extent practicable, to the limited data set (defined in section 164.514(e)(2)) or, if needed , to the minimum necessary information. HITECH mandates that the Secretary issue within 18 months after the date of the statute's enactment guidance on what constitutes "minimum necessary." The required guidance must take into account the guidance on de-identification that is also statutorily required as well as "the information necessary to improve patient outcomes and to detect, prevent, and manage chronic disease." As of the effective date of that guidance, HITECH's provisions prioritizing the use of the limited data set over "minimum necessary" information would no longer apply.

HHS leaves the current regulatory text unchanged because, as the preamble points out, issuance of the required guidance will obviate the need to make any regulatory modifications. ***HHS expresses interest in comments on what aspects of the minimum necessary standard covered entities and business associates believe would find most helpful for HHS to address as well as the types of questions entities may have about how to appropriately determine the minimum necessary for purposes of compliance.***

Direct Application of HIPAA Requirements to Business Associates

Consistent with HITECH, HHS proposes to expand the business associate definition. Simultaneously, HHS proposes to make explicit that certain HIPAA privacy and security rule requirements directly apply to business associates and that business associates and their subcontractors would incur directly liability for their noncompliance with the regulatory requirements.

In addition, HHS proposes to require certain modifications to business associate contracts and other arrangements permissible under the HIPAA rules and to allow for a transition period for bringing certain existing contracts into compliance with the revised business associate provisions.

Expanded business associate definition. HHS proposes to revise the definition of business associate to include the following types of entities:

- ***Patient safety organizations (PSOs).*** As written, the HIPAA rules already would include a PSO as a business associate when the PSO is performing quality analyses and other activities on behalf of a covered health care provider. However, the *Patient Safety and Quality Improvement Act of 2005* (PSQIA) requires that PSOs be treated as business associates under the HIPAA privacy rule; and therefore, HHS proposes to explicitly add PSOs to the business associate definition to more closely align both sets of rules.

  In the preamble, HHS states that a component PSO that performs patient safety activities on behalf of its affiliated covered health care provider would ***not*** be a business associate of the affiliated covered provider. Rather the individuals at the component PSO performing patient safety activities would be workforce members of the covered provider. But where the component PSO contracts out some of its patient safety activities to a third party, that third party would be a business associate of the affiliated covered provider. In contrast, a component PSO that performs patient safety activities for a non-affiliated covered provider would be a business associate of the other covered provider.

  Additionally, because PSQIA deems patient safety activities to be "health care operations" under the HIPAA privacy rule, HHS proposes to reference explicitly patient safety activities, as defined in the PSQIA implementing regulation at 42 CFR 3.20, in the "health care operations" definition. While HHS states that such activities are already encompassed within the definition, which addresses various quality activities, the express reference will "eliminate the potential for any confusion."

- ***Health Information Organizations (HIO), E-Prescribing gateways, and other data transmission organizations.*** As HITECH requires, HHS

proposes to explicitly designate as "business associates" health information organizations, E-prescribing gateways, and other data transmission organizations that transmit protected health information (PHI) to a covered entity (or its business associate) and that require access to such PHI on a routine basis. As the preamble discussion states, data transmission organizations that do not require routine access to PHI would ***not*** be treated as business associates, consistent with previous HHS interpretations that entities that act as mere conduits for the transport of PHI but do not access it other than on a random or infrequent basis are not business associates.

On the other hand, entities that manage the exchange of PHI through a network, including providing patient locator services and performing various oversight and governance functions for electronic health information exchange, would meet the definition because they have "***more than*** random access" to PHI (emphasis added). Moreover, HHS makes clear in the preamble that the specific terms "Health Information Organization" and "E-prescribing Gateway" are merely illustrative of the types of organizations that would fall within the business associate definition.

HHS' proposed definitional change does not explicitly reference the statutory term "Health Information Exchange Organizations" because the Department believes that "Health Information Organization" is the "more widely recognized and accepted term" to describe an organization that oversees and governs the exchange of health-related information among organizations. It also does not reference the statutory term "Regional Health Information Organization" because it is simply an "HIO that governs health information exchange among organizations within a defined geographic area." ***HHS requests comment on the use of these terms and whether additional clarifications or modifications are necessary.***

- ***Vendors of personal health records.*** HHS proposes to designate a vendor that contracts with a covered entity to allow the covered entity to offer a personal health record to patients as part of the covered entity's electronic health record as a business associate, as HITECH requires.

- ***Subcontractors.*** A business associate's subcontractors who "create, receive, maintain, or transmit PHI on behalf of the business associate" also are proposed for inclusion in business associate definition. By doing so, HHS intends that "downstream entities that work at the direction of, or on behalf of, a business associate and handle [PHI] would also be required to comply with the [] Rule[s] in the same manner as the primary business associate, and likewise would incur liability for [] noncompliance."

HHS would define subcontractor as "a person who acts on behalf of a business associate, other than in the capacity of a member of the [business associate's] workforce." As discussed in the preamble, the definition would apply to an agent or other person who acts on behalf of the business associate, "even if the business associate has failed to enter into a [] contract" with the person. However, HHS' proposal would not require the covered entity to have a contract with the subcontractor: the obligation would remain with the business associate to obtain satisfactory assurances in the form of a written contract or other arrangement that the subcontractor will appropriately safeguard PHI. ***HHS requests comment on the inclusion of "subcontractor" and the proposed definition.***

In addition and without changing the meaning of the existing provisions, HHS proposes to move to the business associate definition itself the exceptions from sections 164.308(b)(2) and 164.502(e)(1)(ii)of the current HIPAA rules providing that in certain circumstances a covered entity is not required to enter into a business associate arrangement with the recipient of PHI, such as when a covered entity discloses PHI to health care provider for treatment of an individual.

Explicit limits on business associates' use and disclosure of PHI. HHS proposes to create include an explicit reference to business associates in the section of the privacy rule that lays out the general rules for uses and disclosures of PHI (sec. 164.502(a)). The explicit reference would make clear that, like a covered entity, a business associate may not use or disclose PHI except as permitted or required by the HIPAA privacy or enforcement rules.

Additionally, HHS would add new provisions to this section of the regulations to identify explicitly the permitted and required uses and disclosures of PHI by business associates, stating that business associates:

- ***May use or disclose PHI only as permitted or required by the business associate contract or other arrangements permissible under the rule (sec. 164.504(e)) or as required by law.*** If the covered entity and business associate have failed to enter into a contract or other permissible arrangement, then the business associate may use or disclose PHI ***only*** as necessary to perform its obligations for the covered entity (according to whatever agreement sets the general terms for their relationship) or as required by law; any other use or disclosure would be a violation of the privacy rule. In addition, a business associate would not be permitted to use or disclose PHI in a manner that would violate privacy rule requirements if done by the covered entity. However, a business associate would be permitted to use or disclose PHI for the proper management and administration of the business associate or for the provision of data aggregation services for the covered entity, if such uses and disclosures are permitted by its business associate contract or other arrangement.

- ***Are required to disclose PHI when required by the Secretary to investigate or determine the business associate's compliance*** with applicable regulatory requirements; ***or to the covered entity***, individual, or individual's designee, as necessary to ***satisfy new obligations to comply with individuals' requests for an electronic copy of their PHI***, as discussed previously in this Advisory in the section on the enhanced right of access to PHI in an electronic health record.

HHS also proposes to require that business associates' use, disclose or request for PHI be limited to the minimum necessary information to accomplish the intended purpose of the use, disclosure or request.

As the preamble states, HHS has not added explicit references to "business associate" to other privacy rule provisions that address uses and disclosures by covered entities. According to HHS, such changes are unnecessary, since a business associate generally may only use or disclose PHI in the same manner as a covered entity and, consequently, any limitation in the privacy rule on a covered entity's use or disclose of PHI automatically extends to business associates.

Explicit application of security rule standards to business associates. HHS also proposes to create direct liability for a business associate's noncompliance with the security rule's administrative, physical, and technical safeguards requirements as well as its policies and procedures and documentation requirements, again by referencing "business associate" immediately following "covered entity" in these particular provisions of the regulation text. HHS' proposal is intended implement HITECH's mandate that provisions of the security rule shall apply to business associates in the same manner as these requirements apply to covered entities. HITECH also states that business associates shall be civilly and criminally liable for penalties for violations of these provisions. However, as currently written, none of the security rule's provisions explicitly reference business associates of covered entities.

Moreover, although HITECH does not specifically make reference to the security rule's standard that establishes the general rules applicable to all of the rule's other standards and implementation specifications (sec. 164.306), HHS' proposal includes an explicit reference to business associates in that general provision text. In addition, HHS proposes that, as required of covered entities, business associates must review and modify security measures and update documentation accordingly to maintain compliant security measures.

HHS also would make a technical change to the security rule's administrative safeguards addressable implementation standard for termination procedures for workforce members to recognize that not all workforce members are employees (*e.g.*, some may be volunteers). The current text of the standard refers to

implementing procedures for terminating access to electronic PHI when the employment of a workforce member ends. The revised text would add the words "or other arrangement with" to ensure that the standard includes all workforce members, whether employed or not.

This proposed revision is consistent with HHS' proposal to revise the definition of "workforce member" to make clear that the term includes the employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or a business associate, is under the direct control of respectively, the covered entity or the business associate. The proposed revision to the workforce definition is intended to ensure that covered entities and business associates understand that any obligations the rules impose on them regarding workforce members (*e.g.*, training workforce members on privacy and security policies and procedures, applying sanctions for failure to follow policies and procedures) apply regardless of whether an individual is paid or unpaid for any duties they perform.

Preemption of state law also applies to business associates. Because HITECH requires business associates to comply with certain provisions of the HIPAA rules and also subjects them to penalties for noncompliance, HHS explains that the HIPAA preemption provisions also would apply to business associates. Consequently, HHS proposes to add a reference to business associates in the current regulatory definitions of "contrary" and "more stringent." HIPAA preempts state law requirements that are contrary to a HIPAA standard unless, among other exceptions, the requirement of the state's law is "more stringent" than the contrary HIPAA privacy standard. The current regulatory preemption provisions reference only covered entities and do not mention business associates.

Notably, HHS also proposes to add a reference to HITECH privacy and security provisions in the regulatory text that specifically cites the statutory basis for preemption. HITECH applies the preemption standard to its particular statutory provisions and requirements "in the same manner" as it would apply under the current HIPAA provisions. Thus, HHS' proposed regulatory revision would make clear that HIPAA preemption encompasses HITECH's mandated changes to the privacy and security rules, including the new breach notification obligations.

HHS also uses the publication of the proposed rule to emphasize that the preemption provisions do not create a federal evidentiary privilege and that neither the HIPAA statute nor its implementing regulations give effect to state physician-patient privilege laws or provisions of state law relating to the privacy of individually identifiable health information for use in federal court proceedings. Therefore, consistent with the Supremacy Clause, any state law that was preempted prior to HIPAA because of conflicts with a federal law would continue to be preempted. As the preamble states, "n]othing in HIPAA or its implementing regulations is intended to expand the scope of state laws, regardless of whether they are more or less stringent than federal law."

Requirements to establish business associate relationships with subcontractors. Under the proposed revised rule, business associates would be able to use or disclose PHI only as permitted by the HIPAA rules. Consequently, HHS proposes to add a new section to the privacy rule to permit a business associate to disclose PHI to a subcontractor, and to allow the subcontractor to create or receive PHI on behalf of the business associate, if the business associate obtains satisfactory assurances that the subcontractor will safeguard appropriately the information. HHS also proposes to add a provision to the security rule to allow a business associate to authorize its subcontractors to create, receive, maintain, or transmit electronic PHI only if business associate has a contract or other arrangement in place to ensure a subcontractor will appropriately safeguard the electronic PHI. As a result, the business associate would be required to enter into a compliant contract or other permissible arrangement with all subcontractors, in the same manner that covered entities are required to enter into contracts or other arrangements with their business associates. These proposed changes are intended to align the regulatory requirements with HITECH-specific directive to apply the HIPAA privacy and security standards directly to business associates

As revised, the rules would eliminate the need for covered entities to obtain satisfactory assurances from business associates that are subcontractors. Rather, each subcontractor would be subject to the terms and conditions of a business associate agreement directly with the business associate. As the preamble states, business associates are in the best position to ensure that subcontractors comply with rule requirements. The proposed revisions would not change the parties to the covered entity's business associate contracts and, thereby, ensure that the covered entity does not have a new obligation to enter into separate contracts with subcontractor business associates. Instead, the contractor and subcontractors would be required to obtain business associate agreements with the parties with whom they directly contract for services that involve access to PHI and all business associates and subcontractors would now be business associates with direct liability under the HIPAA rules. Moreover, direct liability under the rules would attach regardless of whether the business associates and subcontractors have actually entered into business associate agreements.

HHS' proposal would eliminate, as unnecessary, the current rule's provision stating that a covered entity that violates the "satisfactory assurances" it provided as a business associate of another covered entity will be in noncompliance with the privacy rule's business associate provisions. Instead, the proposed changes would restrict directly the uses and disclosures of PHI by a business associate, including a covered entity acting as a business associate, to those uses and disclosures permitted by its business associate agreement.

HHS proposes a number of modifications to the business associate agreement requirements in the HIPAA privacy and security rules. First, HHS proposes that business associate agreements must obligate business associates to comply, where applicable, with security rule standards for electronic PHI.

Second, to reflect the new obligation of both covered entities and business associates to provide for particular notifications in the case of breaches of unsecured PHI, HHS proposes to require business associate contracts (in both the relevant HIPAA privacy and security rule provisions) to obligate the business associate to report to the covered entity any breaches of unsecured PHI as required by section 164.410. Consequently, if a breach of unsecured PHI occurs at or by a subcontractor, the proposed revision would require that the subcontractor notify the business associate of the breach, which then must notify the covered entity of the breach. Finally, the covered entity then would notify the affected individuals, the Secretary, and, if applicable, the media, of the breach, unless it has delegated such responsibilities to a business associate.

Third, HHS would insert a new obligation that a business associate that is carrying out any of a covered entity's direct obligations under the rules (*e.g.*, a third party administrator, as a business associate of a group health plan, is distributing the plan's notice of privacy practices to participants) must comply with all requirements that are applicable to the covered entity in the performance of the particular obligation (*i.e.*, to distribute the notice timely). In such instances, the covered entity continues to remain directly liable for failure to meet the required obligation (*e.g.,* providing the notice to individuals in a timely manner) since ultimate responsible under the rule for carrying out the particular obligation (*e.g.*, distributing its notice to plan participants) remains with the covered entity. However, the business associate is contractually liable to the covered entity for the failure. HHS intends the inclusion of the explicit new provision to clarify that a business associate is contractually liable not only for uses and disclosures of PHI, but also for all other requirements of the rule, as they pertain to the performance of the business associate's contract.

Fourth, HHS proposes to eliminate the requirement for covered entities to report to the Secretary when termination of a business associate contract is not feasible. Currently, the regulations deem a covered entity in violation of the business associate provisions if the covered entity knows of a pattern of activity or practice of a business associate that constitutes a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity:

- Took reasonable steps to cure the breach or end the violation, as applicable;
  and
- If such steps were unsuccessful, terminated the contract or arrangement;
  or

- If termination is not feasible, reported the problem to the Secretary.

In light of a business associate's new direct liability for civil money penalties for violations of the HIPAA rules and both a covered entity's and business associate's new obligations to report breaches of unsecured PHI to the Secretary, HHS believes that the department has other ways to learn of a business associate's misuses and breaches of PHI.

HHS also proposes to add a new provision applicable to business associate that mirrors the requirement imposed on covered entities. If a business associate knows of a pattern or practice of activity of its subcontractor that constitutes a material breach or violation of the subcontractor's agreement or other arrangement, the business associate must take reasonable steps to cure the breach or terminate, if feasible, the contract with the subcontractor. As the preamble states, HHS believes this addition to the rule would implement the intent of HITECH to align the obligations of business associates for their subcontractors with the covered entity's obligations for their business associates.

Lastly, HHS also proposes particular changes to streamline the security rules contracting requirements, given that parallel and largely duplicative contracting requirements already are included directly in the privacy rule. As HHS explains, a business associate for purposes of the security rule also is always a business associate for purposes of the privacy rule; and consequently, HHS proposes to remove or otherwise edit appropriately certain current provisions in the security rule. For example, the security rule's current provision (sec. 164.314(a)(2)(ii)) permitting covered entity and business associate that are both governmental entities to have a memorandum of understanding instead of a business associate agreement simply would reference the parallel provision (sec. 164.504(e)(3)) in the privacy rule.

Liability for "agent" business associates. HHS proposes the addition of a provision to make a business associate responsible for the acts of its agents. Like covered entities, a business associate would be liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the business associate, including a workforce member or subcontractor, acting within the scope of the agency.

In addition, HHS proposes a substantive change to the regulatory text related to the liability of covered entities for the acts of their agents, specifically to eliminate the current exception for a covered entity's liability for the acts of its business associate agents where the covered entity:

- Meets the relevant contract requirements;

- Did not know of a pattern or practice of the business associate in violation of that compliant contract; and

- Did not fail to act on business associate violations as the HIPAA rules require.

Essentially, under the proposal, a covered entity would remain liable for the acts of its business associate agents, regardless of whether the covered entity has a compliant business associate agreement in place.

HHS explains that this change is necessary "to ensure, where the covered entity has contracted out a particular obligation under the HIPAA rules, such as the requirement to provide individuals with a notice of privacy practices, that the covered entity remains liable for the failure of its business associate to perform that obligation on the covered entity's behalf." HHS does not believe this proposed change would place any undue burden on covered entities, since they are customarily liable for the acts of their agents under agency common law. Moreover, the preamble states that this change does not create liability for covered entities with respect to business associates that are not agents, *e.g.*, independent contractors. The determination of whether an agency relationship exists with a business association will be based on the facts of the relationship, such as the level of control over the business associate's or subcontractor's conduct.

Requirements for hybrid and affiliated covered entities. HHS proposes to eliminate as unnecessary the rule's current implementation specifications for health care components of hybrid covered entities which obligates a covered entity to ensure that any component that performs business associate-like activities and is included in the health care component complies with the applicable requirements of the HIPAA privacy and security rules. As HHS explains, a covered entity's obligation to ensure that a health care component complies with the privacy and security rules is already set out in a different provision of the current regulation. ***Moreover, in light of a business associate's new direct liability for compliance with certain security and privacy regulatory provisions, HHS also requests comment on whether the rule should require, rather than permit as the current regulatory provision does, a covered entity that is a hybrid entity to include a component that performs business associate-like activities within its health care component so that such components are directly subject to the rules.***

HHS also proposes the addition of a new paragraph that would state clearly that the covered entity itself, and not merely the health care component of a hybrid entity, remains responsible for compliance with regulation's requirements for business associate contracting and other permissible organizational arrangements. As HHS explains, this proposed revision is intended to recognize that hybrid entities may need to execute legal contracts and conduct other organizational matters at the "legal entity" level rather than at the "health care component" level.

Notably, HHS also proposes to remove several specific references throughout the organizational requirements and implementation specifications for both hybrid and affiliated covered entities to make clear that the breach notification requirements also apply to these types of covered entities.

Transition provisions applicable to existing business associate agreements. HHS proposes to relieve some of the burden on covered entities and business associates in complying with the revised business associate provisions by grandfathering certain existing contracts for up to one year beyond the date set for complying with revised final rule. HHS intends that the proposed transition period prevent rushed and hasty changes to thousands of on-going existing business associate agreements while simultaneously allowing covered entities and business associates to continue to function as permitted by the rules until these existing contracts can be revised.

As HHS explains, the proposed transition provisions apply ***only*** to the requirement to amend business associate contracts; they do ***not*** affect any other compliance obligations under the HIPAA rules. For example, beginning on the compliance date of the final revised rule, a business associate may not use or disclose PHI in a manner that is contrary to the privacy rule, even if the business associate's contract with the covered entity has not yet been amended.

The additional transition period would be available to a covered entity or business associate specifically if, prior to the publication date of the final revised rule, a contract or other written arrangement that complies with the prior standards imposed by the HIPAA rules exists and that contract is not renewed or modified between the effective date of the final revised rule and the date required for compliance with the rule's revised substantive provisions (discussed in the final section of this Advisory).

The proposal would grandfather existing written agreements, without regard to whether the agreement conforms to the substantive standards included in the revised final rule. It would grandfather, for example, existing written agreements between business associates and subcontractors that were created to comply with the current rule's existing obligations of business associates to ensure that the "agents" of a business associate agree to the same restrictions and conditions that apply directly to a business associate. These agreements to extracts the specific-required assurances from agents of business associates would be deemed "compliant" with the revised rules until the sooner of either of the following events occur:

- The covered entity or the business associate renews or modifies the contract following the compliance date of the final revised rule;
  or
- The date that is one year after the final revised rule's compliance date.

"Evergreen contracts" (*i.e.*, where a contract renews automatically without any change in terms or other action by the parties) also will be eligible for the extension and deemed compliance for an evergreen contract would not terminate when the contract automatically rolls over. However, the transition provision applies ***only*** to written contracts or other written arrangements, and ***not*** to verbal contracts or other non-written arrangements.

Proposed Changes Related to HIPAA Enforcement

HHS proposes a number of changes to the HIPAA enforcement rule that implement HITECH statutory mandate to conduct investigations of certain complaints about violations of HIPAA requirements and to clarify certain HITECH-imposed levels of culpability and the imposition of civil money penalties for HIPAA violations.

Mandatory investigation where willful neglect involved. As required by HITECH, HHS proposes to make an investigation by the Secretary mandatory for any complaint about a covered entity's (or a business associate's) HIPAA violation when a preliminary review of the facts indicates a possible violation ***due to willful neglect***. Although as a practical matter, HHS currently conducts a preliminary review of every complaint received and proceeds with the investigation in every eligible case where the facts indicate a possible violation, HHS proposes this specific change to make clear its intention to pursue an investigation anytime a factual review indicates willful neglect by a covered entity or business associate.

HHS also proposes to make mandatory that the Secretary conduct a compliance review to determine whether a covered entity or business associate is complying with HIPAA requirements when a preliminary review of the facts indicates a possible violation due to willful neglect. While HITECH's statutory language references complaints and not compliance reviews, HHS suggests that this change "furthers Congress' intent to strengthen enforcement with respect to potential violations due to willful neglect and ensures that investigations, whether or not initiated by complaint, are handled in a consistent manner." As the preamble discussion indicates, if HHS initiates an investigation of a complaint because its preliminary review indicates willful neglect, HHS would not also be required to initiate a compliance review since such activity would be duplicative.

In light of the above proposed changes, HHS also would make clear that it is not required to attempt to resolve cases of noncompliance due to willful neglect by informal means, replacing "will" in the current regulation text with "may." This particular modification would permit HHS to proceed with a willful neglect determination as appropriate. It simultaneously would allow HHS to continue to resolve by informal means complaints and compliance reviews that did not

indicate willful neglect (*e.g.*, where the covered entity or business associate did not know and by exercising reasonable diligence would not have known of a violation, or where the violation is due to reasonable cause). As the preamble discusses, while the particular change in the regulation text would allow the Secretary to proceed directly to a notice of proposed determination without first attempting to resolve the matter informally, it would not alter the fact that during the course of a complaint investigation or a compliance review, a covered entity or business associate would be made aware of, and have the opportunity to address, HHS' compliance concerns.

HHS also proposes to allow the Secretary to disclose PHI obtained in connection with an investigation or compliance review if disclosure is permitted under the Privacy Act at 5 U.S.C. 552a(b)(7). This statutory provision permits disclosure of a record on an individual contained in a statutorily protected system of records to another agency or instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if:

- The enforcement activity is authorized by law;
  and
- The agency has made a written request to the agency that maintains the record.

Under the current HIPAA enforcement regulation, PHI will not be disclosed by the Secretary, except as necessary for determining and enforcing compliance with the HIPAA rules or if otherwise required by law. HHS' proposed revision is necessary to permit the Secretary to cooperate with other law enforcement agencies, such as the State Attorneys General who are permitted under HITECH to pursue actions for HIPAA violations on behalf of their respective state's residents or the Federal Trade Commission, which seeks remedies for violations under other consumer protection authorities.

Clarifications about levels of culpability. While HITECH does not explicitly require modification of the definitions of the any terms associated with the various categories of culpability for HIPAA violations, HHS proposes to amend the definition of "reasonable cause" to clarify the scope of violations fitting within the definition. HHS' proposal would replace the current "reasonable cause" definition with the following:

> An act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.

In the current regulation, "reasonable cause" is defined as "circumstances that would make it unreasonable for the covered entity, despite the exercise of

ordinary business care and prudence, to comply with the administrative simplification provision violated,'' a definition consistent with the Supreme Court's ruling in *United States v. Boyle*, 469 U.S. 241, 245 (1985). But HHS believes that the current definition does not address *mens rea* with respect to one of the HITECH-established categories of violations (*i.e.*, those circumstances in which a covered entity or business associate has knowledge of a violation but lacks the conscious intent or reckless indifference associated with willful neglect).

HHS suggests that the proposed revised definition would continue to recognize those circumstances that would make it unreasonable for the covered entity or business associate, despite the exercise of ordinary business care and prudence, to comply with the particular HIPAA provision violated while simultaneously encompassing those circumstances in which a covered entity or business associate has knowledge of the violation but lacks the conscious intent or reckless indifference associated with willful neglect. The preamble discussion offers two instructive examples:

- A covered entity received an individual's request for access but did not respond within the established regulatory time periods. HHS' investigation reveals that the covered entity received an unusually high volume of requests for access within the time period in question. The covered entity also had compliant access policies and procedures in place and had otherwise responded to the majority of access requests received in that time period in a timely manner. Subsequently, after the period of the violations, the covered entity did respond in a timely manner to all requests for access it received. In this circumstance, while the covered entity had knowledge of the violations, the circumstances would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the provisions it violated. The covered entity also acted in a way that demonstrated a good faith attempt to comply by having compliant policies and procedures in place, responding to the majority of access requests in a timely manner, and otherwise responding to subsequent requests as required. In contrast, the violation might be categorized as being due to willful neglect had the investigation revealed that the series of access requests occurred over a longer period of time, and that the covered entity did not attempt to address the backlog or communicate with the individuals, in writing, regarding the reasons for the delay or the date by which the covered entity would complete its action on the requests.

.

- A covered entity presented for a patient's signature an authorization form to permit a disclosure for marketing purposes that did not contain the core required elements. HHS' investigation reveals that the covered entity was aware of the requirement that an authorization is necessary for the use or disclosure of PHI for marketing and, despite an attempt to draft a compliant authorization, had not included these core elements. In this

circumstance, the covered entity failed to act with the ordinary care and business prudence of one seeking to comply with the requirements of the rule, and therefore, the violation could not be considered to come within the category of violations where the covered entity did not know (and by exercising reasonable diligence would not have known) of the violation. However, it cannot be established that the omission was due to willful neglect involving either a conscious, intentional failure or reckless indifference to the obligation because the covered entity attempted to draft a compliant authorization. Unless otherwise resolved by informal means, HHS would have grounds to find that the violation was due to "reasonable cause."

In addition, while HHS does not propose to otherwise modify the definitions associated with the categories of culpability, the preamble discussion offers additional clarify regarding how the Secretary intends to apply the terms "knowledge," "reasonable diligence," and "willful neglect" to assist covered entities and business associates in tailoring their compliance activities appropriately. Accordingly, hospitals will want to give careful consideration to the preamble discussion on pages 40878 – 40879 in the *Federal Register*.

Specifying factors for use in determining the amount of civil money penalties. After further consideration of HITECH's particular mandates and the significantly broader range of penalty amounts that now may be imposed, HHS would specifically list among the factors the Secretary must consider in determining a civil money penalty amount:

- ***The nature and extent of the violation.*** Moreover, because both circumstances might be indicative measures of "the nature and extent of the violation," HHS would add to this factor "the time period during which the violation(s) occurred" (transferred from another factor in the current regulation text) and "the number of individuals affected".

- ***The nature and extent of the harm resulting from the violation.*** To the current list in this factor for the optional considerations of several specific circumstances which might be indicative of harm, HHS proposes to add "reputational harm," making clear that harm to reputation is as cognizable as physical or financial harm.

HHS would eliminate as redundant from the factors to be considered in determining a civil money penalty amount "the degree of culpability." HITECH creates a statutory system for imposing particular penalty amounts that reflect increasing degrees of culpability for violations.

Moreover, HHS proposes to revise the phrasing in the factor relating to "history of prior compliance" to make it consistent with HHS' existing policy of already considering the general history of HIPAA compliance as a factor in determining

penalty amounts, specifically by substituting the phrase "indications of noncompliance" for the currently used "prior violations" terminology. Generally, as HHS explains, the term "violation" is reserved to circumstances in which HHS makes a formal finding of violation through a notice of proposed determination and refers to a narrower scope of items that HHS' existing policy considers relevant for evaluating compliance history. HHS will now consider, among other factors, whether the current violation is the same or similar to "previous indications of noncompliance" even where there was no "determination" of an actual violation.

Further limits on available affirmative defenses. HHS proposes that, beginning February 18, 2011, the Secretary would be barred from imposing a civil money penalty for a violation of HIPAA's requirements ***only if*** a covered entity or business associate can demonstrate that a permissible statutory criminal penalty for the violation actually has been imposed. Under the proposal, a covered entity or business associate, prior to February 18, 2011, would need to demonstrate only that the violation is criminally "punishable" to bar the Secretary from imposing a civil money penalty. These proposed revisions implement a particular directive from HITECH that the phrase "if the act constitutes an offense punishable" be replaced with "a penalty has been imposed [] with respect to such act." The HITECH directive is specifically effective February 18, 2011.

Prohibition on imposing certain duplicative penalties. HHS also would provide that civil money penalties for the same violation cannot be imposed both under the HIPAA privacy rule and the *Patient Safety and Quality Improvement Act of 2005*. HHS' proposed revision is intended to align the current HIPAA regulatory text, which states that, with limited exceptions, HIPAA's civil money penalties are a "non-exclusive" remedy, with the already effective patient safety statute's specific requirements.

Compliance Dates under the Final Rule and Going Forward

HHS notes that the final rule containing the majority of changes to the HIPAA rules necessitated by HITECH will not take effect until after most of the related provisions of HITECH itself are statutorily effective (*i.e.*, February 18, 2010) and recognizes that it will be difficult to comply with the statutory provisions until after the final rule has been issued. In addition, the department agrees that covered entities and business associates will need some time beyond the final rule's effective date to achieve compliance. As a result, HHS intends to provide covered entities and business associates with 180 days beyond the effective date of the final rule to come into compliance with most of the final rule's provisions.

As noted previously in the section of this Advisory that addresses the proposed changes affecting business associates, the 180-day compliance period ***would***

not govern the time period required to modify particular business associate agreements that qualify for the longer transition period.

In addition, HHS proposes that the general 180-day compliance period for new or modified standards or implementation specifications ***would not apply*** to HIPAA enforcement rule modifications because these provisions "are not standards or implementation specifications" as the terms are defined currently in the HIPAA regulations. As a result, HIPAA enforcement rule-specific modifications would be effective and applicable at the time a final rule becomes effective or as otherwise specifically provided in the particular final rule provision.

Further, for future modifications to the HIPAA privacy and security rules, HHS believes that a 180-day compliance period generally will suffice. Accordingly, HHS proposes to add a new regulatory provision to establish a general compliance date for implementation of new or modified standards to the HIPAA rules. The proposal would make 180 days from the effective date of any such change the time period within which covered entities and business associates must comply with the applicable new or future revisions of the final revised standards or implementation specifications, unless the particular regulatory text explicitly provides for a longer compliance period. ***HHS requests comments on any potential unintended consequences of establishing the 180-day compliance date as a regulatory default.***

Next Steps

The proposed revisions will mean significant changes for hospitals' policy and procedures on the use and disclosure of PHI, including necessitating amendments to the Notice of Privacy Practices. The revisions also will affect any business associate relationships, requiring hospitals to amend existing business associate agreements and to ensure that, as appropriate, compliant provisions are incorporated into future new agreements. Moreover, in light of the proposal that would mandate HHS to conduct investigations of certain complaints about violations of the HIPAA requirements and the additional clarity around certain levels of culpability for violations, hospitals should consider strategically their overall approach to HIPAA compliance.

The release of the proposed rule provides hospitals with an early opportunity for advanced planning to ensure they will be ready to comply with the provisions in the final rule within 180 days of the rule's effective date. Hospitals will want to involve all members of their HIPAA implementation team, including senior managers, legal counsel, privacy and security officers, information technology, human resources, and staff who negotiate and manage relevant outside contractual relationships, in the advance planning efforts.

Finally, please participate in an AHA conference call series on the proposed rule. The first call on Thursday, August 12, at 3 pm ET will examine proposed updates affecting the use and disclosure of PHI, include changes related to marketing, fundraising, sale of data, honoring individual requests to restrict disclosure, and the new right of access to information in electronic records. The second call on Tuesday, August 17, at 3 pm ET will cover issues related to the proposed changes that apply HIPAA requirements directly to business associates of covered entities. Visit http://www.surveymonkey.com/s/783H5TK to register.

Please direct questions and feedback on the proposed rule to Lawrence Hughes, assistant general counsel, at (202) 626-2346 or lhughes@aha.org.