PUBLICATION

HHS Releases Proposed Changes To HIPAA Privacy, Security And Enforcement Rules

August 24, 2010

On July 14, 2010, Secretary Kathleen Sebelius of the United States Department of Health and Human Services (HHS) published notice in the Federal Register of proposed rulemaking[1] aimed at "strengthening" the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy, security and enforcement regulations (collectively referred to as the "HIPAA Rules") and as required by the Health Information Technology for Economic and Clinical Health Act (HITECH Act), which was enacted as a part of the American Recovery and Reinvestment Act of 2009. In highlighting the changes, Secretary Sebelius emphasized that as health information technology systems assist the United States in moving the health care system forward, "the privacy and security of personal health data is at the core of all our work."

Although the proposed rules were expected to implement changes required by the HITECH Act, HHS also took the opportunity to make changes in several areas that were not required by the law. HHS stated that these changes were based on its experience with the privacy, security and enforcement regulations since the original drafting, as well as changes in other laws - including the Patient Safety and Quality Improvement Act of 2005 and the recent Meaningful Use regulations.

The proposed rule includes, among other things, numerous additions to the requirements for business associates and their downstream "subcontractors," several enlightening examples of "willful neglect" and the penalties associated with HIPAA violations, important changes to individual rights requirements, and changes to notices of privacy practices content provisions.

We strongly encourage covered entities and their business associates to submit comments to HHS on these proposed rules. Comments are due on September 13, 2010 and may be submitted by mail or on-line. We have highlighted some areas that are ripe for comment and are happy to assist clients with identifying other issues and drafting comments to address important revisions.

The information below highlights some of the more significant changes proposed by HHS.

BUSINESS ASSOCIATES

Many of the proposed changes to the HIPAA Rules relate to the business associate requirements mandated by the HITECH Act and business associate relationships with agents and subcontractors. HHS proposes changes to the business associate requirements through three primary mechanisms: (1) changes to the definition of "business associate," (2) addition of business associates to the entities that must comply with various provisions of the HIPAA Rules, and (3) changes to the business associate mandatory contract terms.

Expanded Definition of Business Associate

There are three substantive changes proposed to the definition of "business associate." First, as expected, the proposed rule modifies the definition of the term "business associate" to include the entities that Congress (through the HITECH Act) expressly mandated be added. These include health information organizations, e-

prescribing gateways and persons who offer a personal health record to individuals on behalf of a covered entity.

Second, HHS is proposing to make explicit in the regulation that, except when a patient safety organization (PSO) is a component of a covered entity, PSOs must otherwise be treated as a business associate.

Third, HHS also proposes to modify the definition of "business associate" to include subcontractors of business associates. This is an interesting modification in that these downstream entities could be many contracts removed from the covered entity, but yet would still be directly subject to HIPAA under the proposed rule.

Application of HIPAA to Business Associates

HHS proposes to add language to the HIPAA Rules requiring business associates to comply with certain provisions of the Security Rule and making business associates directly liable under the Privacy Rule for failure to comply with the terms of their business associate agreements. Among other things, the proposed rule makes it clear that:

- business associates cannot use or disclose protected health information (PHI) unless permitted or required by the Privacy or Enforcement Rule;
- use and disclosure of PHI by business associates is permissible only if allowed by the Privacy Rule, required by the business associate agreement, or required by law; and
- business associates must comply with the minimum necessary standard with regard to uses and disclosures of PHI.

Changes to Mandatory Business Associate Agreement Terms

The proposed rule also requires covered entities to amend their business associate agreements to add specific contract terms. Among other mandatory terms, under the proposed rule, business associate agreements must:

- require that business associates comply with the Security Rule with regard to electronic PHI;
- notify the covered entity of a breach of unsecured PHI; and
- ensure that any subcontractors that create or receive PHI for the business associate agree to the same restrictions and conditions that apply to the business associate.

Business associate agreements must also require the business associate to enter into a written contract or other arrangement that complies with the Privacy Rule with any subcontractors to whom the business associate discloses PHI. Business associate subcontractors, in turn, are required to obtain business associate contracts or other HIPAA-compliant arrangements with their subcontractors, thus creating a chain of direct accountability.

Although business associate subcontractors are by definition considered "business associates" under the proposed rule, covered entities are not required to execute a business associate agreement directly with a business associate's subcontractor. Rather, only the business associate would be required to obtain a business associate agreement with its subcontractor.

Even if a covered entity does not obtain a business associate agreement with all the mandatory terms, the business associate is still directly liable under the HITECH Act. The covered entity, however, could face a penalty for failure to obtain a HIPAA-compliant agreement with its business associate, and a business associate could face a penalty for failure to obtain a business associate agreement with its subcontractor, if applicable.

Issues for Comment: Business Associate Provisions

- The business associate agreement amendment requirements will likely be the subject of much comment because many covered entities had hoped that costly contract amendments would not be expressly required, but rather, that the HITECH Act business associate provisions would be implemented by operation of law. Other covered entities, seeking in good faith to comply with the February 17, 2010 compliance date (with no formal guidance from the Office of Civil Rights [OCR] and with state enforcement looming) have already amended their business associate agreements. Amendments have taken the form of everything from full scale revision to the use of a general catchall provision stating that the business associate will comply with the HITECH Act requirements. But, these amended business associate agreements may not contain the exact language noted in the proposed rules. Commenters may wish to seek clarification regarding whether such amendments satisfy the new business associate contract requirements if they are in substantial compliance with the intent of the law.
- The addition of "subcontractors" to the definition of the term "business associate" and to the written business associate agreement requirements is a regulatory expansion of the express HITECH Act requirements. If this definition is finalized, business associate subcontractors will be considered business associates with direct liability (as well as contractual liability) and expensive regulatory obligations under the law.

AUTHORIZATIONS

A covered entity (and a business associate under the proposed rule) generally may use and disclose PHI without an individual's authorization only for the specific purposes set forth in the Privacy Rule. The Privacy Rule currently provides two specific circumstances, subject to certain exceptions, in which an authorization always must be obtained: most uses and disclosures of psychotherapy notes, and uses and disclosures for "marketing" purposes. The proposed rule, following the mandate of the HITECH Act, adds the sale of PHI (defined as receiving direct or indirect remuneration in exchange for making the PHI available) as a third circumstance that requires authorization unless one of several exceptions applies. Additionally, the proposed rule eases certain requirements for authorizations used in the context of research and participation in clinical trials.

Requiring Authorizations for Sale of PHI

Under the proposed rule, covered entities (and business associates) must obtain an authorization for any disclosure of PHI in exchange for direct or indirect remuneration. The authorization has to state expressly that the disclosure will result in remuneration to the covered entity (or to the business associate, although it seems unlikely that most covered entities would allow for the sale of PHI). Note that, with respect to the recipient of the information, if PHI is disclosed for remuneration by a covered entity or business associate to another covered entity or business associate, the recipient covered entity or business associate cannot redisclose the PHI in exchange for remuneration, unless a valid authorization is obtained with respect to such redisclosure.

The exceptions in the HITECH Act and proposed rule under which receipt of remuneration is acceptable, even absent an individual's authorization, are:

- certain public health activities,
- certain research purposes as long as the price charged for the information reflects the costs of preparation and transmittal of the data,
- treatment of the individual,

- business transactions (sale, transfer, merger, or consolidation and related due diligence) of a covered entity,
- payment for services rendered under a business associate agreement,
- providing an individual with access to his or her PHI pursuant to the individual's request for access, and
- such other purposes as the Secretary determines to be necessary and appropriate by regulation.

The proposed rule adds two exceptions not set out in the HITECH Act. One is for disclosures that are "required by law," a term that is defined in the Privacy Rule. HHS explains that the exception is proposed to ensure that a covered entity can continue to disclose PHI where required by law, even if the covered entity receives remuneration for the disclosure. The other is to except from the authorization requirements a disclosure of PHI for 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 or is a fee otherwise expressly permitted by other law.

Easing of Compound Authorization Requirements for Research

The Privacy Rule generally requires authorization for use and disclosure of PHI for research purposes, and it has generally prohibited "compound authorizations" in which an authorization for the use and disclosure of PHI is combined with any other legal permission. The Privacy Rule does, however, permit the combining of 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. The Privacy Rule does not currently permit the combining of authorizations that condition treatment, payment, enrollment in a health plan, or eligibility for benefits with an authorization for another purpose for which these activities may not be conditioned.

HHS has received a number of comments suggesting that allowing a covered entity to combine conditioned and unconditioned authorizations would streamline the process for obtaining an individual's authorization for research, make the documentation responsibilities of these covered entities more manageable, and result in an authorization that would be simpler and thus more meaningful to the individual (in contrast to the individual receiving multiple forms, which may be confusing).

The proposed rule, therefore, allows a covered entity to combine conditioned and unconditioned authorizations for research, provided that the authorization clearly:

- differentiates between the research components that constitute a condition of treatment from those that do not, and
- allows the individual the option to opt in to the unconditioned research activities.

These provisions allow, for instance, a covered entity to combine an unconditioned 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 an authorization.

Issues for Comment: Authorizations for Future Research Use and Disclosure

- whether the Privacy Rule should permit an authorization for uses and disclosures of PHI for future research purposes to the extent such purposes are adequately described in the authorization, such that it would be reasonable for the individual to expect that his or her PHI could be used or disclosed for such future research;

- whether the Privacy Rule should permit an authorization for future research only to the extent the description of the future research included certain elements or statements specified by the Privacy Rule, and if so, what should those be; and
- whether the Privacy Rule should permit the first option above as a general rule but require certain disclosure statements on the authorization in cases where the future research may encompass certain types of sensitive research activities, such as research involving genetic analyses or mental health research, that may alter an individual's willingness to participate in the research.

MARKETING

Since the promulgation of the Privacy Rule, the term "marketing" has been defined to mean "the making of a communication about a product or service that encourages recipients of the communication to purchase or use the product or service." The definition is subject to certain exceptions for communications pertaining to health care operations or treatment. If a communication satisfies an exception, it can be made without obtaining the individual's authorization for any use or disclosure of the person's PHI in making the communication.

Under the proposed rule, the general construct described above and core definition of "marketing" would remain intact. The exceptions to the definition of marketing, however, would undergo substantial modifications, many of which were dictated by the HITECH Act. The impact of the more substantive changes made in the proposed rule to the exceptions to the definition of marketing are as follows:

- An authorization is required for a covered entity to send a communication for the purpose of health care operations if the covered entity receives or has received financial remuneration in exchange for making the communication.[2]
- An authorization is not required for a covered health care provider to send a communication for the purpose of treatment provided that:

    1. the covered health care provider's notice of privacy practices includes a statement informing individuals that the provider may send treatment communications to the individual concerning treatment alternatives or other health-related products or services where the provider receives financial remuneration from a third party in exchange for making the communication and provides the individual with a right to opt-out of receiving such communications; and
    2. the treatment communication itself discloses the fact of remuneration and provides the individual with a clear and conspicuous opportunity to elect not to receive any further such communications.
- An authorization is not required for refill reminders provided that any financial remuneration received by the covered entity in exchange for making the refill reminder communication is reasonably related to the covered entity's cost of making the communication.

Issues for Comment: Refill Reminders

HHS has requested comment on the scope of the refill reminder exception; specifically, whether communications about drugs that are related to the drug currently being prescribed (e.g., adjunctive therapies) should fall within the exception. HHS is also considering whether to require that a covered entity only receive financial remuneration for making such a communication to the extent it did not exceed the actual cost to make the communication, but is concerned about the burden of calculating the costs of making each communication. Therefore, HHS requests comment on the types and amount of costs that should be allowed under this provision.

In addition to the above, the proposed rule provides guidance on the opt-out requirement and the difference between communications for treatment and health care operations.

Opt-Out Requirement for Subsidized Treatment Communications

The proposed rule prohibits covered entities (or business associates) from causing the individual to incur an undue burden or more than a nominal cost in exercising his or her right to opt-out of subsidized treatment communications. HHS indicated that the use of 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 would be acceptable. It noted, however, 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.

Issues for Comment: Opt-Out Requirement

HHS requests comment on the following:

- How should the opt-out apply to future subsidized treatment communications? Further, should the opt-out prevent all future subsidized treatment communications by the provider or just those dealing with the particular product or service described in the current communication?
- What is the workability of requiring that health care providers—who intend to send subsidized treatment communications—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 the requirement?

Treatment Versus Health Care Operations

The proposed rule emphasizes the difference between treatment communications and communications for health care operations purposes.

Communications by health plans concerning health-related products or services included in a plan of benefits or for case management or care coordination are never considered treatment for purposes of the Privacy Rule, but rather would always be health care operations and require individual authorization under the proposed rule if financial remuneration is involved.

Subsidized communications by a health care provider about health-related products or services for case management or care coordination or to recommend alternative treatments or settings of care depend on how the provider makes the communication. For example, a covered health care provider that 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. 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. The provider would be making a communication for health care operations if it does not receive any financial remuneration for the communication, but would be making a communication for marketing if it does receive financial remuneration.

Issues for Comment: Marketing

Recognizing the difficulty in making judgments as to which communications are for treatment purposes and which are for health care operations purposes and the need to avoid unintended adverse consequences to a covered health care provider's ability to provide treatment to an individual, HHS requests comment on the proposed changes to the marketing rule as well as the alternatives of excluding treatment communications altogether even if they involve financial remuneration from a third party or requiring individual authorization for both treatment and health care operations communications made in exchange for financial remuneration.

FUNDRAISING

The proposed rule makes a number of changes to the regulations governing a covered entity's use or disclosure of PHI for fundraising activities. First, the opt-out provision is strengthened by requiring that a covered entity provide, with each fundraising communication sent to an individual, a clear and conspicuous opportunity for the individual to elect not to receive further fundraising communications. The election cannot cause the individual to incur an undue burden or more than nominal cost. HHS has suggested the use of a toll-free phone number or an e-mail address and has stated that requiring the individuals to write and send a letter to the covered entity asking not to receive future fundraising communications would constitute an undue burden on the individual for purposes of this proposed requirement.

Second, a covered entity cannot condition treatment or payment on an individual's choice not to receive fundraising communications. Election not to receive fundraising communications is treated as a revocation of authorization under the Privacy Rule. A covered entity must make "reasonable efforts" to ensure that those individuals who have opted out of receiving fundraising communications are not sent such communications.

Third, covered entities that intend on contacting individuals to raise funds must still include a statement to that effect in their notice of privacy practices, but the notice of privacy practices must inform individuals that they have a right to opt out of receiving such communications, as discussed below.

Issues for Comment: Fundraising

HHS indicated that there have been concerns regarding the prohibition on the use or disclosure of certain treatment information without an authorization, such as the department of service where care was received and outcomes information. Covered entities have complained that the prohibition harms their ability to raise funds and prevents them from targeting their fundraising efforts and avoiding inappropriate solicitations to individuals who may have had bad treatment outcomes. HHS seeks comment on:

- whether the Privacy Rule should allow additional categories of protected health information to be used or disclosed for fundraising, such as department of service or similar information, and if so, what those categories should be;
- the adequacy of the minimum necessary standard to appropriately limit the amount of PHI that may be used or disclosed for fundraising purposes; or
- whether the current limitation should remain unchanged.

HHS also requests comments on whether, if additional categories are allowed, covered entities should be required to provide individuals with an opportunity to opt out of receiving any fundraising communications before making the first fundraising solicitation.

NOTICE OF PRIVACY PRACTICES

The proposed rule requires that additional statements be included in a covered entity's Notice of Privacy Practices (NOPP). The NOPP is required to include a statement that describes when an authorization is necessary for the disclosure of psychotherapy notes or for marketing activities; a statement that other uses and disclosures not described in the NOPP will only be made with the individual's written authorization; and a statement that the authorization may be revoked in writing.

The NOPP must inform individuals if a health care provider intends to send communications concerning treatment alternatives or health-related products or services where the provider receives a financial remuneration (either directly or indirectly) and provide information on the right to opt out of receiving such

communications. Likewise, a covered entity that intends to contact individuals to raise funds must inform individuals in the NOPP of the intention and of their right to opt out of receiving the communications. The provision of an opt-out option is a fertile area for comment as covered entities are likely to face significant operational and administrative challenges implementing the requirement.

The proposed changes to the NOPP do not include a specific statement regarding notification to affected individuals, the media, or the Secretary following a breach of unsecured protected health information.

Issues for Comment: NOPP

HHS has asked for public comment on whether the rules should require a specific statement in the NOPP on breach notification. HHS has also stated that because of the financial burden dissemination of a new NOPP places on health plans, it is requesting comment on options for health plans to timely inform individuals of the proposed changes to the NOPP. Because health care providers are required to make the NOPP available upon request and at the delivery site, HHS believes they do not face the same financial burden.

MINIMUM NECESSARY STANDARD

The HITECH Act required the Secretary to issue guidance on the "minimum necessary" standard within 18 months after the date of enactment in February 2009. In the interim, covered entities are required to determine whether they can limit uses and disclosures to a "limited data set" or employ their traditional minimum necessary policies. Given the pending guidance, no modifications to the regulatory text on the "minimum necessary" standard are proposed, except to make it applicable to business associates when they use, disclose or request protected health information.

Issues for Comment: Minimum Necessary Standard

HHS, in the proposed rule, requests public comment on what guidance on minimum necessary would be beneficial.

INDIVIDUAL RIGHTS

The proposed amendments to the rules also would change how covered entities and business associates must respond to certain individual rights with respect to protected health information.

Patient Requests to Restrict Disclosure

The Privacy Rule provides individuals with a right to request that a covered entity restrict uses or disclosures of PHI for treatment, payment, and health care operations purposes, as well as for disclosures to family members and certain others. Under the current Privacy Rule, covered entities are not required to agree to such requests for restrictions, but if a covered entity does agree to restrict the use or disclosure of an individual's PHI, the covered entity must abide by that restriction, except in emergency circumstances when the information is required for the treatment of the individual. The HITECH Act, however, requires that when an individual requests such a restriction on disclosure, the covered entity must agree to the requested restriction (unless otherwise required by law) if:

- the request regards disclosures of PHI to a health plan for the purpose of carrying out payment or health care operations; and
- the restriction applies to PHI that pertains solely to a health care item or service for which the provider has been paid out-of-pocket in full.

The proposed rule addresses this requirement but acknowledges that it may not be as straightforward as it first appears due to the web of treatment interactions between covered entities, business associates and individuals.

Issues for Comment: Individual Rights

- HHS seeks comment on whether a restriction placed upon certain PHI should continue to attach to such information as it moves downstream and asks for suggestions of methods through which a provider could use information technology to facilitate such notice.
- Covered entities may also wish to comment on whether it is administratively and contractually feasible to limit disclosure to payors and how these proposed requirements could cause the covered entity to violate mandatory disclosure terms the covered entities have agreed to in their managed care and other payor participation agreements.

Patient Access to PHI

Under the Privacy Rule currently, individuals generally have a right to review or obtain copies of their PHI, to the extent it is maintained in a covered entity's designated record set. The HITECH Act strengthens this right by providing that when a covered entity uses or maintains an electronic health record with respect to PHI of an individual, the individual (a) has a right to obtain a copy of such information in an electronic format and (b) may direct the covered entity to transmit such copy directly to the individual's designee, provided that any such choice is clear, conspicuous, and specific.

The HITECH Act would apply the above provisions only to PHI in an electronic health record, which is defined to mean "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff." HHS seeks to expand the definition of electronic health record to all PHI maintained electronically in designated record sets, whether or not the designated record set is an electronic health record (as defined by HITECH). HHS cites the need to avoid a complex set of disparate requirements for access to PHI in electronic health records versus other types of electronic records systems.

The proposed rule requires covered entities and business associates to provide an individual with access to his or her electronic information in the electronic form and format requested by the individual, if it is readily producible, or in a readable electronic form and format as agreed to by the covered entity and the individual if the requested form and format is not readily producible. This is an expansion of the current Privacy Rule, which does not require negotiating with an individual if a requested form or format is not readily producible.

Note that unlike providing copies of paper PHI, for which a covered entity or business associate may charge a reasonable fee that includes elements such as supplies (paper, toner, etc.) and copier depreciation, any fee imposed for providing such an electronic copy generally must not be greater than the entity's labor costs in responding to the request.

The proposed rule also provides that, if requested by an individual, a covered entity or business associate must transmit the copy of PHI directly to another person designated by the individual. The proposed rule requires satisfaction of the "clear, conspicuous, and specific" requirement through a written request from the individual. The Privacy Rule already allows for electronic documents to qualify as written documents for such purpose and for electronic signatures to satisfy any requirements for a signature, to the extent the signature is valid under applicable law; therefore, the process could be either electronic- or paper-based.

Currently, a request for disclosures must be approved or denied, and, if approved, access or a copy of the information provided, within 30 days of the request, with an additional 30 days if the records are only accessible from an off-site location and a one-time 30-day extension in extenuating circumstances.

Issues for Comment: Access

Recognizing the expectation and capacity to provide individuals with almost instantaneous access to PHI in electronic form, HHS hints that it is considering adopting a different timeliness standard for electronic PHI and seeks comment on an appropriate standard.

ENFORCEMENT

The HITECH Act altered and expanded HHS's enforcement functions. Not only did the law make business associates directly liable for violations of the Security Rule and certain provisions of the Privacy Rule, it also called for a shift in the agency's enforcement of the HIPAA Rules. Historically, HHS's enforcement had largely been based on voluntary compliance. As a result of the HITECH Act, however, the enforcement framework now focuses more heavily on the imposition of penalties.

On October 30, 2009, HHS issued an Interim Final Rule (IFR) that revised the Enforcement Rule to incorporate those provisions of HITECH Act (§ 13410(d)) that took immediate effect. These included setting forth four categories of violations that reflect increasing levels of culpability, the corresponding tiers of civil monetary penalty (CMP) amounts, and the revised limitations on the Secretary's authority to impose penalties. As summarized below, the current proposed rule seeks to revise various provisions of the Enforcement Rule, as amended by the IFR.

Proposed Changes Mandating Conduct by HHS

The HITECH Act included provisions that require the Secretary to take certain actions when willful neglect on the part of a covered entity or business associate is suspected or identified. To implement these provisions, HHS has proposed changes to the Enforcement Rule that:

- require the Secretary to investigate any and all complaint(s) of a violation, if a preliminary investigation of facts indicates that a purported violation was due to willful neglect;
- unless it has already begun to investigate a complaint, require the Secretary to conduct compliance reviews to determine if a covered entity or business associate is complying with applicable administrative simplification provisions when a preliminary investigation of facts indicates that a purported violation was due to willful neglect; and
- mandate that the Secretary impose a CMP for violations due to willful neglect.

The proposed rule provides several insightful examples of conduct that OCR would consider to constitute "willful neglect." These include the following:

- a covered entity failed to have a proper disposal policy and procedure and hard drives with electronic PHI were disposed of in an unsecured dumpster;
- a covered entity failed to respond to an individual's request for a restrictions and an investigation showed the lack of a policy and procedure on restriction requests and a general refusal to accept restrictions from individuals who request restrictions; and
- a covered entity failed to report a breach as required by the breach notification rule when an unencrypted laptop was lost.

When willful neglect is not indicated, the proposed rule makes clear that the Secretary has discretion to use informal means to investigate and resolve complaints and compliance reviews.

Expanded Authority for HHS to Disclose PHI

Under existing rules, the Secretary has authority to disclose PHI obtained from covered entities and business associates in an investigation or compliance review when necessary for determining and enforcing compliance with the HIPAA Rules or if otherwise required by law. HHS is proposing to allow the Secretary to disclose PHI if permitted under the Privacy Act at 5 U.S.C. § 552a(b)(7). This expanded authority enables HHS to cooperate with other law enforcement agencies, such as state attorneys general or the Federal Trade Commission, when pursuing HIPAA actions for state residents or other remedies under consumer protection laws.

Clarification of Intent Standard for Reasonable Cause

The HITECH Act and the IFR set forth increasing levels of culpability for violations, including: (i) "did not know," (ii) "reasonable cause," (iii) "willful neglect – corrected," and (iv) "willful neglect – not corrected." In the proposed rule, HHS stated that there is no clear delineation of intent between reasonable cause and willful neglect. The proposed rules amend the definition of reasonable cause to make clear that the category applies when there is knowledge (either actual or imputed), but the violation lacks conscious intent or reckless indifference.

Addition of Business Associate to Enforcement Rule Provisions

The proposed rule adds the term "business associate" where necessary and appropriate to effectuate the imposition of liability on business associates for violations of the Privacy and Security Rules.

Increased Exposure for Acts/Omissions of Agents

HHS is seeking to remove the exception for principal liability for covered entities so that the covered entity remains liable for acts of business associate agents, regardless of whether the covered entity has a compliant business associate agreement in place. Thus, a covered entity would remain liable for the failure of a business associate to perform a HIPAA obligation on behalf of the covered entity (e.g., issuance of a Notice of Privacy Practices). The proposed rule also would empower HHS to impose CMP liability against the business associate for acts or omissions of its agents when acting within the scope of agency.

Addition of Factors to Be Considered in Determining a CMP

The Enforcement Rule sets forth certain factors to be considered in determining the amount of a CMP. The proposed rule amends the structure and content of the factors to be considered. The changes include, for example, requiring the Secretary to consider (i) the nature and extent of the violation (e.g., number of individuals affected; time period during which the violation occurred); (ii) the nature and extent of harm resulting from the violation (e.g., reputation harm); and (iii) the history of prior compliance (as opposed to only considering prior violations) with the HIPAA Rules.

Narrowing of Affirmative Defenses

The proposed rule implements HITECH Act § 13410(a)(1), which, as of February 18, 2011, bars the Secretary from imposing a CMP on a covered entity or business associate if a criminal penalty has been imposed under 42 U.S.C. § 1320d-6 for the conduct at issue. The proposed rule also makes clear that, for violations prior to

February 18, 2011, it is an affirmative defense if a covered entity or business associate establishes that the violation is merely criminally punishable under 42 U.S.C. § 1320d-6.

COMPLIANCE DATES

The proposed rule provides for varying dates of compliance, as follows:

- The effective date for compliance with revised business associate agreement provisions is one year beyond the compliance date of the final rule. (The general compliance date of the final rule is 180 days from the rule's effective date.) This additional one-year transition period is available only if prior to the compliance date of the final rule, the covered entity or business associate had an existing contract or other written arrangement that complied with prior provisions of HIPAA and the agreement or arrangement was not renewed or modified between the effective date and the compliance date for modifications to the HIPAA Rules. Evergreen contracts would be eligible for the extension to the compliance date.
- The prohibition on sale of PHI would apply to disclosures occurring 180 days after the date of promulgation of the final rule.
- The Enforcement Rule provisions are effective upon promulgation of the final rule, except where otherwise expressly provided (e.g., affirmative defenses).
- For all others, the general compliance date is 180 days after the date of promulgation of the final rule.

MISCELLANEOUS PROVISIONS

Decedents

The Privacy Rule requires covered entities, and now business associates, to protect the privacy of a decedent's PHI generally in the same manner and to the same extent that is required for the PHI of living individuals. The proposed rule limits this protection to a period of 50 years following an individual's death and modifies the definition of "PHI" to make clear that the individually identifiable health information of a person who has been deceased for more than 50 years is not PHI under the Privacy Rule.

The proposed rules also permit disclosure of a decedent's information to family members and others who were involved in the care or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

Issues for Comment: Decedents

Covered entities may wish to express their views on whether the 50 year decedent requirement is burdensome.

School Immunizations

The proposed rule adds provisions regarding authorizations for disclosure of immunization records to a school. In this regard, covered entities would be permitted to disclose proof of immunization to schools in states that have school entry or similar laws, and written authorization would no longer be required as long as the covered entity obtains agreement, which may be oral, from a parent or guardian (or from the student, if the individual is an adult or emancipated minor).

Issues for Comment: School Immunization Provisions

Recognizing the potential for miscommunication and later objection by the parent in the absence of written authorization, HHS requests comment on whether the Privacy Rule should require that a provider document oral agreements or whether a requirement for such documentation would be overly cumbersome.

WHAT IS NOT ADDRESSED

HHS did not address HITECH Act changes to the accounting of disclosure requirements or the state attorneys general's new authority to enforce the HIPAA Rules. HHS also does not modify or finalize the Interim Final Breach Notification Rules, which have been in effect since September 23, 2009.

Comments on any of the above issues are due on September 13, 2010 and may be submitted by mail or on-line. If you would like assistance in submitting comments or have questions about any of these issues, contact your Baker Donelson attorney or any of the attorneys in the Health Law Group.

---

1. 75 Fed. Reg. 40,686 (July 14, 2010).

2. Under the proposed rule, the term "financial remuneration" means "direct or indirect payment from or on behalf of a third party whose product or service is being described." Direct or indirect payment does not include any payment for treatment of an individual. HHS emphasized that financial remuneration for purposes of the definition of "marketing" must be in exchange for making the communication itself and be from, or on behalf of, the entity whose product or service is being described.