ALERT
August 3, 2010

HEALTH LAW
News Concerning
Recent Health Law Issues

COZEN O'CONNOR
www.cozen.com

# PROPOSED NEW RULES IMPLEMENTING HITECH AMENDMENTS TO HIPAA MAKE SIGNIFICANT CHANGES

Salvatore G. Rotella, Jr. • 215.665.3729 • *srotella@cozen.com*
Katherine M. Layman • 215.665.2746 • *klayman@cozen.com*
Gregory M. Fliszar • 215.665.7276 • *gfliszar@cozen.com*
Melanie K. Martin • 215.665.2724 • *mmartin@cozen.com*
Judy Wang Mayer • 215.665.4737 • *jmayer@cozen.com*

On July 14, 2010, the Department of Health and Human Services ("HHS") issued a Notice of Proposed Rulemaking (the "Proposed Regulations") to modify certain regulations that implement the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Specifically, the Proposed Regulations implement statutory amendments to HIPAA's Privacy, Security, and Enforcement Rules made by the Health Information Technology for Economic and Clinical Health Act ("HITECH"), which was enacted as part of the American Reinvestment and Recovery Act of 2009 in February of last year. The Proposed Regulations represent significant revisions to HIPAA and have major implications for all covered entities (i.e., health care providers, health plans, and health care clearinghouses), as well as for business associates and their subcontractors. HHS previously issued interim final regulations implementing certain limited provisions of HITECH on August 24, 2009 (regarding breach reporting requirements) and October 30, 2009 (regarding civil monetary penalties).

In sum, the most important substantive aspects of the Proposed Regulations are as follows:

- **Preemption:** HIPAA and its regulations do not create any new privileges applicable to federal court proceedings.
- **Hybrid entities:** In the case of hybrid entities, the covered entity itself and not just its designated health care component must comply with the Security Rule provisions regarding business associate arrangements and other organizational requirements.
- **Business associates:** Business associates (defined to include their subcontractors) are now directly liable for compliance with the Security and Privacy Rules. While they are not required to maintain policies and procedures documenting their compliance with the Privacy Rule, they must perform a security risk assessment and adopt Security Rule policies and procedures.
- **Marketing:** Previously, covered entities did not need to get an authorization to make certain treatment- and health-related communications with patients encouraging them to purchase or use a product or service. Such unauthorized communications are no longer permissible if the covered entity receives money for making them, although it may continue to send unauthorized refill reminders and treatment communications in exchange for payment, if it meets certain notice and opt out requirements.
- **Sale of protected health information ("PHI"):** A covered entity or business associate may not receive direct or indirect remuneration in exchange for the disclosure of PHI, unless the covered entity/business associate obtains a valid authorization from the individual or the disclosure is among those included on a list of enumerated exceptions to the rule.
- **Research:** Researchers may now obtain from study participants a single, compound authorization for the disclosure of PHI for both: (i) research-related treatment conditioned upon the individual's participation in the study; and (ii) corollary research purposes for which treatment may not be conditioned, such as tissue banking. Such compound authorizations must clearly differentiate between the two types of activities and must permit the participant to opt in to the "unconditioned" research activity.

- **Fundraising:** The basic fundraising rule remains the same, although the Proposed Regulations strengthen an individual's right to control the use of his or her PHI for fundraising purposes.
- **Notice of privacy practices:** A covered entity's mandatory Notice of Privacy Practices must now include: (i) a description of the uses of PHI that require authorization; (ii) a statement regarding certain marketing and treatment communications the covered entity intends to send to individuals; and (iii) a statement that the covered entity must agree to restrict disclosures of PHI to an individual's health plan for services for which the individual has paid the covered entity in full.
- **Health plan disclosure restrictions:** A covered entity must agree to an individual's request to restrict disclosure of his or her PHI to his or her health plan, if: (i) the disclosure is for the purpose of carrying out payment or health care operations; and (ii) the PHI pertains solely to a health care item or service for which the individual, or someone on the individual's behalf (other than the health plan), has paid the covered entity in full.
- **Individuals' access to PHI:** The Proposed Regulations strengthen individuals' right of access to all PHI maintained in one or more designated record sets electronically, regardless of whether the designated record set at issue constitutes an electronic health record; and
- **HIPAA enforcement and civil monetary penalties.** HHS must conduct its own, proactive compliance review if a preliminary assessment of the facts indicates a potential statutory violation due to willful neglect. The Proposed Regulations, however, also narrow the scope of violations that are deemed to be due to willful neglect, and thus would result in mandatory civil monetary penalties.

This Health Law Alert addresses each of these topics in more detail below.

HHS has indicated that it will delay enforcement of many of the new rules included in the Proposed Regulations. Perhaps most notably, covered entities and business associates will have until 6 months after the effective date of the forthcoming finalized version of the regulations to comply with most of the new provisions implementing HIPAA's Privacy and Security Rules. The final rule, moreover, will not go into effect until the late fall of 2010 at the very earliest, as HHS is accepting comments on the Proposed Regulations through September 13, 2010 and has historically taken significant time to issue final rules. The new regulations that implement HIPAA's Enforcement Rule, by contrast, would generally be effective immediately upon issuance of the final rule. Covered entities and business associates will also generally have an additional 12 months, and thus up to 18-months after the effective date of the final rule, in which to bring their business associate agreements into conformance with the new regulations. Any modifications to the agreements or affirmative renewals they undertake prior to expiration of the 18-month transition period, however, must comply with the new regulations as set forth in the final rule.

## Preemption

HHS proposes to clarify the HIPAA provisions regarding the preemption of state law. The Proposed Regulations clarify that the HIPAA statute and its implementing regulations neither create a federal evidentiary privilege nor make State physician-patient privilege laws (or provisions of State law relating to the privacy of individually identifiable health information) applicable to federal court proceedings. In short, any state law that was preempted prior to HIPAA because of conflicts with a federal law would continue to be preempted. As with other portions of the proposed rule, HHS proposes to modify the preemption provisions so that they apply directly to business associates as well as to covered entities.

## Hybrid Entities

The Proposed Regulations clarify certain issues relating to hybrid entities—i.e., covered entities whose business activities include both covered and non-covered functions, and that designate health care components in accordance with certain provisions of the Privacy Rule. Most notably, HHS clarifies that, with regard to hybrid entities, the covered entity itself (i.e., the legal entity), and not just a designated health care component of the covered entity, must comply with the Security Rule provisions regarding business associate arrangements and other organizational requirements. *HHS has requested comments as to whether a covered entity that is a hybrid entity should be required (rather than permitted) to include a component that performs business associate-like activities within its health care component, which would now make that component directly subject to the Privacy and Security Rules.*

## Business Associates

HITECH fundamentally changed the responsibilities of business associates ("BAs") with respect to HIPAA. Prior to HITECH, BAs were subject to HIPAA compliance pursuant only to the terms of their business associate agreements ("BAAs") with covered entities. HITECH, however, now makes BAs directly subject to compliance with most of the HIPAA requirements. Significantly, any entity deemed to be a BA must comply with HIPAA, regardless of whether the BA is itself party to a BAA.

The Proposed Regulations set out the parameters of these requirements as follows:

- **Security Rule.** BAs must comply with the Security Rule's administrative, physical, and technical safeguard requirements, and must have the policies, procedures and documentation required by that rule. Performing and documenting a security risk assessment is a time-consuming and challenging process that is a fundamental obligation under the Security Rule, and one that most BAs probably have not undertaken to date. The implications of this and other new steps BAs must now take to comply with the Security Rule are likely to significantly complicate contract negotiations between covered entities and BAs.
- **Privacy Rule.** The Proposed Regulations clarify the somewhat ambiguous language of HITECH by requiring BAs to comply with the use and disclosure requirements of the Privacy Rule to the same extent as covered entities. BAs, however, will not be required to have detailed policies and procedures, as they must under the Security Rule, or to designate a Privacy Officer. Nonetheless, because BAs will be subject to direct enforcement for violations of both rules, it makes sense for them to take some steps—perhaps short of formal policies and procedures—to demonstrate meaningful internal standards and compliance efforts they follow to meet their obligations under the Privacy Rule. In addition, BAs must:
  - Comply with the minimum necessary standard; and
  - Take reasonable steps to cure any breach caused by a subcontractor.

In a surprising development, the Proposed Regulations define "business associate" to include subcontractors of BAs. Given the complex and costly nature of Security Rule compliance, this change will likely make negotiations with subcontractors significantly more challenging for BAs. It also raises the question of how far downstream (e.g., through multiple layers of subcontractors) the new requirements will extend. We anticipate that HHS will further clarify the obligations of subcontractors in the final version of the regulations.

Finally, CMS has provided for a generously long transition period for parties to revise existing BAAs. Thus, covered entities and BAs may continue to operate under existing BAAs for up to 18 months after the effective date of the final rule. This grandfathered status applies to BAAs in place prior to the publication date of the final rule, so long as the BAAs were HIPAA compliant at that time and are not modified between 60 and 240 days after publication of the final rule.

## Marketing

According to HHS, HITECH reflected Congressional concern that covered entities were taking advantage—for commercial gain—of certain exceptions to HIPAA's general prohibition on the unauthorized use of PHI for marketing purposes. To curtail these practices, the Proposed Regulations change the definition of marketing so as to limit the exceptions and tighten the restrictions on the unauthorized use of PHI to sell products or services.

HIPAA has historically required covered entities to obtain valid authorizations from individuals before using or disclosing their PHI to market to them. Marketing is defined as making "a communication about a product or service that encourages the recipients of the communication to purchase or use the product or service." 45 C.F.R. § 164.501. HIPAA, however, also provided for exceptions to the general ban, and thus did not require authorization prior to using a patient's PHI, for: (1) communications relating to health-related products or services provided by or included in the plan benefits of the covered entity; (2) treatment-related communications; or (3) communications for case management, care coordination, or to recommend alternative treatments, providers, or care settings.

Through HITECH, Congress cut back on these exceptions and provided that health-related communications by a covered entity do not qualify as health care operations—and thus *would* require prior authorization—if the entity gets paid for making the communication. The Proposed Regulations implement these statutory amendments through the following changes to the regulatory definition of marketing found at 45 C.F.R. § 164.501:

- The existing exceptions to "marketing," and thus to the requirement that a covered entity obtain prior authorization from the patient, are retained for communications (1) describing a health-related product or service and (2) for case management or care coordination, or recommending alternative treatments, providers, or care settings, *provided* the covered entity does not receive financial remuneration (i.e., direct or indirect payment, not including payment for treatment of the individual, from or on behalf of third party whose product or service is being described) for making the communication;
- Refill reminders or other communications about a drug or biologic currently prescribed to an individual will not constitute marketing, *provided* any financial remuneration for the communication is reasonably related to the covered entity's cost of making the communication. (*Note that HHS solicited comments regarding the proper scope of this exception, such as whether information regarding generic alternatives or new formulations of the drug qualify for this exception*;) and
- Communications for treatment of an individual also will not constitute marketing, *provided* that if the communication is in writing and the provider receives financial remuneration in exchange, the provider meets certain notice and opt-out requirements. (As to the mechanism for opting out of future communications, HHS noted that requiring individuals to write and send an opt-out letter would be unacceptably burdensome.)

Finally, certain other communications between a covered entity and an individual that have historically not required an authorization—such as face-to-face communications about products or services, and communications promoting health in general—are unaffected by the Proposed Regulation and continue not to constitute marketing.

## Sale of PHI

HITECH added the sale of PHI to the list of circumstances that require a HIPAA authorization. To implement that provision, the Proposed Regulations would prohibit a covered entity or business associate from receiving direct or indirect remuneration in exchange for the disclosure of PHI, unless the covered entity/business associate obtains a valid authorization from the individual or the disclosure is among those included on a list of enumerated exceptions to the rule.

Specifically, a proposed new 45 C.F.R. § 164.508(a)(4)(i) would require that a covered entity or business associate obtain an authorization for any disclosure of PHI in exchange for direct or indirect remuneration from or on behalf of the recipient of the PHI. In addition, the proposed rules require that the authorization must specifically state that the covered entity is receiving direct or indirect remuneration in exchange for the PHI. According to HHS, mandating such a statement will ensure that individuals can make informed decisions as to whether they wish to authorize disclosure of their PHI when the disclosure will result in remuneration to the covered entity.

Further, HHS explains that if the recipient of the PHI disclosed in exchange for remuneration is a covered entity or business associate, it could not re-disclose the PHI in exchange for remuneration unless a valid authorization is obtained in accordance with proposed section 164.508(a)(4)(i). *HHS is requesting comments on both the proposed authorization requirement and its re-disclosure position*.

Under the Proposed Regulations, however, the new authorization requirement will not apply to disclosures:

- For public health activities pursuant to §164.512(b) or §164.514(e);
- For research activities pursuant to § 164.512(i) or § 164.514(e), where 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 research purposes;
- For treatment and payment purposes pursuant to § 164.506(a);
- For the sale, transfer, merger or consolidation of all or part of the covered entity and for related due diligence;
- To or by a business associate for activities that the business associate undertakes on behalf of a covered entity pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate for the performance of such activities pursuant to a business associate contract;
- To an individual, when requested under the access and accounting provisions of the Privacy Rule (sections 164.524 and 164.528);
- Required by law as permitted under § 164.512(a); and
- Permitted by and in accordance with the applicable requirements of the Privacy Rule, where 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 a fee otherwise expressly permitted by other law.

*HHS is requesting comments on the proposed exceptions to this "sale of PHI" authorization requirement and whether any additional exceptions should be included in the final rule.*

## Research

In the preamble to the Proposed Regulations, HHS acknowledges that in addition to research-related treatment, research often also involves a corollary research activity, such as using or disclosing PHI to contribute to a central research database or tissue repository. The Privacy Rule currently requires separate authorizations for each research activity. In response to concerns raised by the research community, HHS is now proposing to permit compound authorizations, if certain conditions are met, and is also seeking comments regarding the authorization process for future research studies.

**Compound Authorizations.** Currently, the Privacy Rule allows a covered entity to condition the provision of research-related treatment on the signing of an authorization for the use of the individual's PHI, but prohibits so-called "compound authorizations," in which a researcher combines authorization for the use and disclosure of PHI with other legal permission. 45 C.F.R. §§ 164.508(b)(4)(i) & 164.508(b)(3). A narrow exception allows a researcher to combine an authorization to use/disclose PHI in a research study with another written permission (e.g., informed consent) for the same study, but that exception does not extend to combining an authorization that conditions treatment (e.g., participation in a clinical trial) with an authorization for another purpose for which treatment may not be conditioned (e.g., tissue banking). Thus, for example, covered entities must currently obtain separate authorizations from research subjects for participation in a clinical trial and for the collection of specimens for a tissue repository.

The research community has expressed concern that requiring multiple authorizations hampers research and that multiple forms could be confusing for potential subjects. HHS agreed that allowing a covered entity to combine research authorizations would generally streamline the process and lessen the documentation burdens for providers conducting research. As a result, the Proposed Regulations would amend 45 C.F.R. § 164.508(b)(3)(i) and (iii) to allow a covered entity to combine conditioned and unconditioned research authorizations, provided that the authorization:

- Clearly differentiates between the conditioned, research-related treatment and the corollary unconditioned, research activity; *and*
- Allows the individual to opt in to the unconditioned research activities.

The Proposed Regulations clarify that this exception includes combining an authorization for the use and disclosure of PHI with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or tissue repository, or with a consent to participate in research. Thus, covered entities would be able to use a single document to obtain consent for participation in a clinical research trial, the use of PHI in the clinical trial, and the storage of the participant's PHI and/or biological specimens in a data bank or repository.

HHS notes that while the proposed modifications do not alter the core elements and required statements for a valid HIPAA authorization, covered entities would have some flexibility in structuring compound authorizations. A covered entity, for example, could meet the proposed compound authorizations requirements by: (i) describing the unconditioned research activity on a separate page of the authorization; (ii) using a check box for the unconditioned research activity to signify whether the individual chose to opt in, with a separate signature line for the overall authorization; or (iii) providing a distinct signature line to authorize participation in the optional research. *HHS is requesting comments on additional methods that could be used to clearly describe and differentiate the conditioned and unconditioned research activities covered by a compound authorization.*

**Future Research.** Research often involves obtaining health information and biological specimens to create a research database or tissue repository that is maintained for unspecified future research studies. HHS has interpreted the current Privacy Rule, however, to require that authorizations for the use and disclosure of PHI for research purposes be study-specific to comply with 164.508(c)(1)(iv), which requires an authorization to include a description of each purpose of the requested use or disclosure. This interpretation was based in part on HHS' concern that individuals presented with an authorization that does not clearly describe potential future research would lack information essential to make an informed decision about whether to sign the authorization.

The research community expressed concerns that this interpretation impedes secondary research by requiring

covered entities to re-contact individuals to sign multiple authorizations for future research studies. It also appears to differ from the current practice under the federal "Common Rule" for the protection of human subjects found at 45 C.F.R. Part 46. In response to these concerns, HHS is considering modifying its position that an authorization for research purposes must be study specific. *HHS is requesting comments on a number of proposed options, including their impact on the conduct of research and patient understanding of authorizations.* The proposed options include:

- Permitting an authorization to encompass future research purposes, to the extent that the authorization adequately describes such purposes so that it would be reasonable for an individual reading the description to expect that his or her PHI could be used for such future research;
- Permitting an authorization for future research purposes only to the extent the description of the future research includes certain elements or statements specified in the Privacy Rule, and if so, what those required elements and/or statements should include;
- Permitting the first option above as a "general rule," but requiring that the authorization include specified disclosure statements if the future research involves sensitive activities such as genetic analyses or mental health research.

HHS notes that any such modifications would not alter an individual's ongoing right to revoke his or her authorization for future research at any time and that the authorization would have to include a description of how to effect such a revocation. *HHS requests comments on how such a revocation would work with respect to future research studies.*

## Fundraising

The Proposed Regulations do not fundamentally change the existing rule that a covered entity may use or disclose limited PHI (i.e., an individual's demographic information and the dates of health care provided to the individual) to an institutionally-related foundation or BA without the individual's authorization, so long as: (i) the Notice of Privacy Practices contains such a notification; and (ii) the fundraising materials sent to the individual contain an explanation of how the individual may opt out of future fundraising materials.

The Proposed Regulations make the following tweaks to the existing rule, however, which are designed to strengthen an individual's ability to opt-out of fundraising activities:

- The opt-out notification must accompany each fundraising communication, and must be clear and conspicuous;
- The opt-out requirements must not be burdensome or impose undue cost. HHS interprets this to mean that individuals should be given the opportunity to email or call a toll-free number to opt-out, and should not have to write and mail a letter;
- A provider may not condition future treatment on an individual's choice with respect to receiving fundraising communications; and
- A covered entity may not send future fundraising communications to an individual who has opted out. (The current rule merely provides that the covered entity must make reasonable efforts not to send future fundraising communications.)

*HHS is soliciting comments about certain details of the fundraising rule, including:*

- *To what fundraising communications should the opt-out apply? For example, is the opt-out limited to the specific campaign at issue or does it apply to all future fundraising campaigns?*
- *Should the demographic information covered entities are permitted to use to identify potential donors be expanded to include the patient's department of service (e.g., surgery or oncology)? As to this latter comment request, it is clear that HHS has been besieged by providers who have tried to explain that many satisfied patients would actually welcome the opportunity to make a donation to their hospital or other provider.*

## Notice of Privacy Practices

The Privacy Rule currently requires most covered entities to have and distribute a notice of privacy practices ("NPP") that describes permitted uses and disclosures of PHI, the covered entity's legal duties and privacy practices regarding PHI, and the individual's rights concerning PHI. Providers are required to make a materially revised NPP available upon request on or after the effective date of the revision. Health plans, however, must provide notice to individuals covered by the plan within 60 days of any material revision to a NPP.

The Proposed Regulations would require a covered entity to materially change its NPP in several respects.

*First*, the NPP would have to include a description of the uses and disclosures of PHI that require an authorization (uses and disclosures of psychotherapy notes, PHI for marketing purposes for which the covered entity receives remuneration, and the sale of PHI) and a statement that other uses and disclosures not described in the NPP will be made only with the individual's authorization.

*Second*, the Proposed Regulations would require the NPP's description of uses and disclosures regarding treatment, payment, and health care operations to include a separate statement regarding certain marketing and treatment communications if the covered entity intends to send such communications to the individual. Specifically, if a covered entity intends to (i) send treatment communications to the individual concerning treatment alternatives or other health-related products or services where the provider receives financial remuneration for making the communication or (ii) contact the individual to raise funds for the covered entity, the NPP must inform the individual of the communications and that he/she has the right to opt out of receiving such communications.

*Third*, the Proposed Regulations would require the NPP's statement that the covered entity is not required to agree to an individual's request to restrict certain uses and disclosures of PHI to include an exception for restrictions on certain disclosures to health plans, as set forth immediately below.

## Health Plan Disclosure Restrictions

The Privacy Rule currently permits an individual to request a restriction on the use or disclosure of his/her PHI by a covered entity, but does not require the covered entity to agree to such request. The Proposed Regulations, by contrast, require a covered entity to agree to a restriction on the disclosure of PHI to a health plan, provided that: (i) the disclosure is for the purpose of carrying out payment or health care operations; and (ii) the PHI pertains solely to a health care item or service for which the individual, or someone on the individual's behalf (such as a family member, but not the health plan), has paid the covered entity in full. A covered entity, for example, must honor a request from a patient to not disclose PHI to a health plan concerning his/her diabetes-related treatment as long as the individual, or someone on the individual's behalf, pays the covered entity in full for the care. Under those circumstances, the covered entity is also prohibited from disclosing the patient's PHI to a business associate of a health plan.

Notwithstanding the individual's request to restrict disclosure, the Proposed Regulations would permit a covered entity to disclose PHI to a health plan if such disclosure is required by law, or if the individual fails to pay for the item or care. With respect to disclosures for payment issues, HHS states that it expects covered entities to make reasonable efforts to resolve the payment issue with the individual, such as by notifying the individual and providing him/her an opportunity to pay, before disclosing the PHI to the health plan for payment. *HHS requests comments on the extent to which covered entities must make reasonable efforts to secure payment from the individual.*

In the event a patient requests a health plan disclosure restriction and then seeks follow up for which he/she does not request a restriction and asks the provider to bill the health plan, HHS recognizes that the provider may need to submit information about the original treatment to the health plan to facilitate payment of the follow up care. Here, HHS states that it would consider the lack of a restriction with respect to the follow up care to extend to any PHI necessary to effect payment for that care, even if the PHI pertained to prior treatment that was subject to a restriction.

Finally, the Proposed Regulations modify the provisions regarding terminating and documenting restrictions to clarify that the current termination and documentation provisions related to restrictions also apply to health plan disclosure restrictions, and that a covered entity may not unilaterally terminate a health plan disclosure restriction.

*Due to the myriad of treatment interactions between covered entities and individuals, and the practical challenges of implementing the health plan disclosure restriction, HHS seeks comments on various issues, including: (i) the obligation of a provider subject to a restriction to inform other providers downstream of the restriction: (ii) restrictions and the use of an automatic prescribing tool (e.g., a provider electronically sends a prescription to a pharmacy for an individual who has requested a restriction and the pharmacy, which is unaware of the restriction, sends billing information to the plan before the patient arrives to pick up the prescription); and (iii) how the provision will function with respect to HMOs, which generally prohibit providers from accepting payment directly from their enrollees.*

## Individuals' Access to PHI

The Privacy Rule currently establishes, with limited exceptions, an enforceable means by which individuals

can review or obtain copies of their PHI, to the extent such information is maintained in the designated record set of a covered entity. Although the right of individuals to access their PHI exists regardless of the format of the PHI, HITECH strengthens the Privacy Rule's right of access to PHI that is used or maintained specifically in an electronic health record ("EHR"). To avoid disparate requirements for access to PHI in EHRs versus other types of electronic records systems, HHS proposes to apply the new access requirements to all PHI maintained in an electronic designated record set, regardless of whether the record set is maintained in an EHR.

The Privacy Rule currently requires a covered entity to provide an individual with access to PHI in the form requested by him/her, if it is readily producible in that form, or, if not, in a readable hard copy form or other form agreed to by the covered entity and the individual. HITECH expanded this requirement by expressly requiring a covered entity that uses or maintains an EHR to provide the individual with a copy of such information in an electronic format. The Proposed Regulations reconcile these provisions by requiring a covered entity that electronically maintains PHI in a designated record set to provide the individual with an electronic copy of such information in the electronic form or format requested or in an otherwise agreed upon form. Thus, while an individual's right of access to an electronic copy of PHI is currently limited by whether the form or format requested is readily producible, the Proposed Regulations would require covered entities that maintain such information electronically to provide some type of electronic copy if requested by the individual.

HHS recognizes that the foregoing requirement may bind covered entities to standards that are not yet technically feasible. It therefore proposes to permit covered entities to make some other agreement with individuals as to an alternative means by which they may provide a readable copy, to the extent the requested format is not readily producible.

HITECH also provided that an individual may direct the covered entity to transmit an electronic copy of PHI in an electronic record directly to an entity or person designated by the individual. The Proposed Regulations seek to expand this right by making it expressly applicable to PHI in paper *or* electronic format, and requiring the individual's request to be "clear, conspicuous, and specific," in writing, and signed by the individual.

As for costs related to producing a copy of PHI, the Privacy Rule currently permits a covered entity to impose a reasonable, cost-based fee, which may include the cost of the supplies for, and labor of, copying the PHI, postage associated with mailing the PHI, and the preparation of an explanation or summary of the PHI if agreed to by the individual. HITECH limited the allowable costs by providing that a covered entity may not charge more than its labor costs in responding to the request for the copy. The Proposed Regulations reconcile these requirements as well, by permitting a covered entity to charge for the labor for copying PHI whether in paper or electronic form, the cost of supplies for creating the paper copy or electronic media, if the individual requests that the electronic copy be provided on portable media, and the cost of postage, if the individual requests that the covered entity mail the portable media containing the PHI. With respect to charging for labor for producing PHI electronically, HHS makes clear that while covered entities may charge a reasonable cost for labor to review the access request and produce the electronic copy, a covered entity may not charge a standard "retrieval fee" that does not reflect the actual labor costs associated with the retrieval of the electronic information.

*Lastly, HHS requests comment regarding an appropriate, common timeliness standard for the provision of access to electronic records.* Although HITECH did not amend the timeliness requirements for provision of access, HHS recognizes that with the advance of electronic health records, there is an increasing expectation and capacity to provide individuals with almost instantaneous electronic access to PHI. *Thus, HHS requests comment on aspects of existing systems that would create efficiencies in processing of requests for electronic information, whether the current standard could be altered for all systems, paper and electronic, such that all access requests should be responded to within 30 days, whether (contrary to HHS' assumption) a variety of timeliness standards based on the type of electronic record is preferable, the time necessary for covered entities to review access requests and determine appropriateness, and whether the provision permitting an extension for access to PHI maintained off-site should be eliminated altogether.*

## Enforcement and Penalties

HITECH also made various important changes to how HIPAA is enforced and how statutory violators are penalized. Significantly, § 13410 of HITECH established the

following four-tiers of increasing civil monetary penalties corresponding to the culpability associated with a violation:

- The first, and lowest, tier is for violations in which the person did not know, and by exercising due diligence, would not have known that he or she violated a provision of the statute;
- The second tier is for violations in which the violation was due to reasonable cause and not willful neglect;
- The third tier is for violations that were due to willful neglect but that were timely corrected; and
- The fourth tier is for violations that were due to willful neglect and were not timely corrected.

HHS implemented some of the HITECH amendments relating to enforcement through the Interim Final Rule it issued on October 30, 2009. The Proposed Regulations implement additional aspects of the HITECH amendments that relate both to enforcement and monetary penalties.

## Enforcement

HITECH requires HHS to impose a civil monetary penalty for any violation involving willful neglect and to conduct a mandatory investigation whenever a preliminary review of the facts of a complaint filed with HHS indicates a possible violation due to willful neglect. The Proposed Regulations likewise require HHS to conduct its own, proactive mandatory compliance review whenever a preliminary review of the facts indicates a possible violation due to willful neglect. Under the new rule, HHS retains discretion to conduct investigations of complaints and proactive reviews under circumstances not implicating violations due to willful neglect.

Prior to HITECH, HIPAA required HHS to attempt to reach an informal resolution of violations it uncovered in response to complaints or its own compliance reviews. The Proposed Regulations now state that HHS may seek such informal resolutions at its discretion, and thus is not required to attempt to resolve by informal means instances of noncompliance due to willful neglect.

## Penalties

**Reasonable Cause.** Perhaps the most significant change to the penalty structure in the Proposed Regulations is to the definition of "reasonable cause," as used in connection with the second tier of culpability for violations. That term was previously 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." 45 C.F.R. § 160.401. The Proposed Regulations, however, define "reasonable cause" as

> 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.

Under the prior definition, any knowing violation automatically ended up in the third or fourth/willful neglect tiers, for which civil monetary penalties are mandatory. That is no longer the case. Under the new definition of "reasonable cause," a covered entity that is aware of the relevant rule and fails to act with ordinary care and business prudence, but does not display the type of intentional conduct or reckless indifference that amounts to willful neglect, may still fall within the second culpability tier, for which civil monetary penalties are not mandatory. As an example, the preamble to the Proposed Regulations posits a hypothetical in which a covered entity was aware of the rule that it obtain a signed authorization prior to making disclosures for marketing purposes, but nonetheless presented a patient with an authorization form that did not meet all of the regulatory requirements under the Privacy Rule. Under the new scheme, this violation may still fall within the second tier.

As HHS makes clear in the above hypothetical and others, it is crucial for covered entities to maintain effective policies and procedures, and document its compliance with the same, to avoid a finding that it acted with "willful neglect."

**Agency.** Under HIPAA, a covered entity was already subject to liability for a violation of the Privacy Rule by its business associate, if the latter was deemed to be acting as an agent of the former. Consistent with the fact that HITECH generally makes business associates subject to the Privacy Rule in much the same fashion as covered entities, the Proposed Regulations also provide that a business associate is liable, in accordance with the federal common law of agency, for a civil monetary penalty for a violation based on the act or omission of *its* agent, including a workforce member or subcontractor, acting within the scope of the agency. Whether a business associate is an agent of a covered entity, and whether a

subcontractor is an agent of a business associate, is based on the facts of the relationship, such as the level of one's control over the other.

In addition to expanding agency liability to business associates based on the conduct of their subcontractors, the Proposed Regulations also eliminate a prior exception that applied to covered entities. Under the previous regulatory scheme, a covered entity was not liable even for the acts or omissions of a business associate that constituted the covered entity's agent, if the requirements of the Business Associate Agreement had been met, and the covered entity did not know of a pattern or practice of the business associate in violation of that agreement and fail to act to address any such pattern or practice of which the covered entity became aware. To ensure that a covered entity remains liable for the failure of a business associate to perform a particular obligation under HIPAA that the covered entity contracts out to the business associate, the Proposed Regulations do away with this exception.

**Determination of Penalty Amounts.** Finally, the Proposed Regulations expand upon and re-organize the factors HHS will consider in assigning a violation to a particular culpability tier. In addition to establishing the four tiers of culpability for violations, HITECH directed HHS to base determination of civil monetary penalty amounts on "the nature and extent of the violation and the nature and extent of the harm resulting from such violation." The Proposed Regulations amend the structure of the relevant regulation (45 C.F.R. § 160.408), which already includes many of the relevant factors, and makes explicit the added HITECH statutory requirement. Among other things, the regulations direct HHS to consider the "number of individuals affected" in determining the "extent of the violation," and to consider "reputational harm" in determining the "nature and extent of harm resulting from the violation." The Proposed Regulations also clarify and update the availability of various affirmative defenses to the imposition of civil monetary penalties.

*For further information regarding the Proposed Regulations, please contact any of the authors of this Alert or any of the attorneys in the Cozen O'Connor Health Law Practice Group.*