

Client Alert

Latham & Watkins
Corporate Department

HHS Proposes Regulations to Implement the HITECH Act's Expansion of HIPAA Requirements

On July 8, 2010, the US Department of Health and Human Services (HHS) announced proposed changes to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security and Enforcement Rules. These changes are designed to implement the statutory amendments to HIPAA made by the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to conform the HIPAA Privacy Rule to the Patient Safety and Quality Improvement Act of 2005, and to propose other changes that will improve the workability and effectiveness of the HIPAA Rules. The Notice of Proposed Rulemaking (NPRM) that contains the proposed changes was published in the Federal Register on July 14, 2010, and comments must be submitted to HHS by September 13, 2010.

Major changes to the HIPAA Rules proposed by HHS in the NPRM are summarized below. Although many of the HITECH Act's requirements became effective on February 18, 2010, HHS will give covered entities, business associates and their subcontractors 180 days after the final rule is published to comply with its provisions. In the NPRM,

HHS also proposes to establish a 180-day compliance period for all future modifications to the HIPAA Privacy and Security Rules, except as otherwise provided.

HIPAA Requirements Apply to Business Associates and Their Subcontractors

The HITECH Act requires that certain of HIPAA's privacy and security standards are directly applicable to covered entities' "business associates" — independent contractors of those covered entities who receive or obtain protected health information (PHI) in connection with providing a service on their behalf. The NPRM implements this requirement by revising existing regulations applicable to covered entities to also include references to "business associates." It also revises the definition of "business associate" to include Patient Safety Organizations, vendors of personal health records and entities that provide data transmission services with respect to PHI and require routine access to such PHI, such as Health Information Organizations and E-Prescribing Gateways. The NPRM goes a step further than the HITECH Act, however, and also proposes to

"HHS proposes to expand the HIPAA Rules to regulate anyone servicing the health care industry who has access to PHI, including downstream subcontractors of business associates who have no direct relationship to a covered entity."

define “business associate” to include subcontractors of a business associate, which consist of any downstream entities that work at the direction or on behalf of a business associate and handle PHI. These downstream entities would not have a direct relationship with the covered entity, but would still be required to comply with HIPAA standards or be subject to civil and criminal penalties in the same manner that these penalties would apply to the covered entity. The business associate on whose behalf the subcontractor is working would be responsible for obtaining the required satisfactory assurances (through a contract or other arrangement) from the subcontractor to protect the privacy and security of the PHI.

In short, HHS proposes to expand the HIPAA Rules to regulate anyone servicing the health care industry who has access to PHI, including downstream subcontractors of business associates who have no direct relationship to a covered entity. Since the HITECH Act became effective, covered entities and business associates have been modifying their agreements with each other in order to comply with the new requirements. If this proposal in the NPRM is finalized, agreements between business associates and their subcontractors must also be similarly modified.

Recognizing that it may be administratively difficult to quickly modify such contracts, the NPRM provides for a transition period to “grandfather” certain existing contracts for a period of up to one year beyond the compliance date of the final rule. This “grandfathering” provision would apply to contracts between covered entities and business associates, as well as contracts between business associates and subcontractors, if, prior to the publication date of the final rule, these entities had an existing contract or other written arrangement that complied with the prior provisions of the HIPAA Rules,

and such contract or arrangement was not renewed or modified between the effective date and the compliance date of the final rule.

Increased Enforcement Provisions

HHS proposes several changes that will strengthen the enforcement of HIPAA's privacy and security standards. For example, the NPRM implements the HITECH Act's requirement that the Secretary of HHS conduct a compliance review or formally investigate a complaint where a preliminary review of the facts indicates a possible violation due to willful neglect. The NPRM also makes clear that a covered entity remains liable for the acts of its business associates who act as agents of the covered entity (as opposed to independent contractors), regardless of whether the covered entity has a compliant business associate agreement in place. Further, the NPRM proposes that the Secretary of HHS must consider the nature and extent of the violation as well as the nature and extent of the harm resulting from the violation, in addition to the factors enumerated in Section 1128A of the Social Security Act, when determining civil penalty amounts. These proposed changes, if finalized, will likely lead to increased HIPAA enforcement activity.

Limitations on the Use of PHI for Marketing Purposes

The use of PHI for marketing communications (*i.e.*, communications about a product or service that encourage recipients to purchase or use the product or service), is generally prohibited without authorization of the individual, unless an exception applies. These exceptions include communications made for the treatment of an individual and communications for the purpose of health care operations (*e.g.*, communications by a health plan

regarding health-related products or services that are included in its plan benefits). Such communications are not considered to constitute marketing communications and, therefore, an authorization is not required before using PHI to make them. The HITECH Act now limits these exceptions with regard to communications for which a covered entity receives financial remuneration.

The NPRM implements these new limitations by proposing that communications for the purpose of health care operations for which financial remuneration is received are marketing communications that require individual authorization. With regard to communications for treatment purposes for which a provider receives financial remuneration, although an authorization would not be required, HHS proposes to require a provider to notify individuals through its Notice of Privacy Practices that a provider intends to send such subsidized treatment communications to an individual, and that the individual has an opportunity to opt out of receiving them.

The NPRM proposes to define “financial remuneration” as direct or indirect payment from or on behalf of a third party whose product or service is being described, excluding direct or indirect payment for the treatment of an individual. Thus, these new limitations on the use of PHI for marketing communications where financial remuneration is received would apply differently depending on whether a communication is for the purpose of health care operations or for the purpose of treatment.

In addition, HHS proposes to include a specific exception mandated by the HITECH Act for communications about a drug or biologic that is currently being prescribed for the individual (*e.g.*, refill reminders) for which financial remuneration is received by the covered entity for making the

communication, provided that the financial remuneration is reasonably related to the covered entity’s cost of making the communication. The use of PHI for such communications would not require individual authorization.

Prohibition of the Sale of PHI Without Individual Authorization

The HITECH Act imposes a new requirement that PHI may not be sold without individual authorization, except in certain circumstances. The NPRM implements this statutory provision by proposing that a covered entity must obtain an authorization for any disclosure of PHI in exchange for direct or indirect remuneration. The authorization must state that the disclosure will result in remuneration to the covered entity. Also, a recipient of such PHI cannot re-disclose the PHI in exchange for remuneration unless a valid authorization is obtained. An individual authorization would not be required if PHI is sold for the following purposes: (1) public health activities; (2) research purposes; (3) treatment and payment purposes; (4) health care operations, including disclosures relating to the sale, transfer, merger or consolidation of a covered entity; (5) disclosure to a business associate for activities that the business associate undertakes on behalf of a covered entity, as long as the only remuneration provided is by the covered entity to the business associate for the performance of such activities; (6) disclosures to an individual when access to an individual’s PHI is requested under 45 C.F.R. § 164.524 or an accounting is requested under 45 C.F.R. § 164.528 and a reasonable cost-based fee is imposed; (7) disclosures required by law under 45 C.F.R. § 164.512; (8) disclosures permitted by 45 C.F.R. Part 164, Subpart E, 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; and (8) disclosures made for permissible purposes for which the covered entity received remuneration that was consistent with applicable state law.

Limitations on the Use of PHI for Fundraising Purposes

The HIPAA Privacy Rule permits a covered entity to use or disclose to a business associate or an institutionally related foundation certain PHI for its own fundraising purposes without an individual's authorization, provided that an individual is notified of this possibility through a covered entity's Notice of Privacy Practices, and is given an opportunity to opt out of receiving such communications. The NPRM proposes to strengthen an individual's ability to prevent such communications by requiring that a covered entity provide, with each fundraising communication sent, a clear and conspicuous opportunity for the individual to elect not to receive further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than nominal cost. HHS also proposes to require that a covered entity may not condition treatment or payment on an individual's choice with respect to receiving fundraising communications, and that a covered entity may not send fundraising communications to an individual who has elected not to receive such communications.

Compound Authorizations for Research Purposes

The NPRM proposes to permit a covered entity to combine authorizations for the use and disclosure of PHI for multiple purposes in a research project into a single authorization, if all of the purposes relate to the research

project. If finalized, this proposal would simplify the process by which research institutions acquire authorizations from research subjects during clinical trials, which currently involves securing separate authorizations for each use or disclosure of PHI. For example, a covered entity would be able to combine an authorization permitting the use and disclosure of PHI associated with a specimen collection for a central repository with an authorization permitting the use and disclosure of PHI for clinical research that conditions research-related treatment on the execution of a HIPAA authorization. HHS has also requested comment on whether and how an authorization could be used to permit the use of PHI for future potential research studies.

PHI of Deceased Individuals

The NPRM proposes to amend the HIPAA Privacy Rule to require a covered entity to comply with its requirements with regard to a deceased individual's PHI for a period of 50 years following the date of death. The definition of PHI would also be amended to make clear that it does not include individually identifiable information of a person who has been deceased for more than 50 years. Currently, covered entities must protect the privacy of a decedent's PHI generally in the same manner and to the same extent that is required for PHI of living individuals. HHS explains that this proposal would address the difficulty of obtaining authorizations from decedents' personal representatives as time passes, yet still protect the privacy interests of most living relatives of the decedent or other affected individuals. In addition, the NPRM proposes to permit covered entities to disclose a decedent's information to family members and others who were involved in the care or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

Disclosure of Immunization Records to Schools

To facilitate a child's entry into school, HHS proposes to permit covered entities to disclose proof of immunization, without a written authorization, to schools in states that have laws that prohibit a child from attending school unless the school has proof that the child has been appropriately immunized. Although written authorization would not be required, a covered entity must still obtain agreement (verbal or otherwise) from a parent, guardian or other person acting *in loco parentis* for the child.

Definition of "Minimum Necessary"

The HIPAA Privacy Rule requires covered entities to limit uses and disclosures of, and requests for, PHI to the "minimum necessary" to accomplish the intended purpose of the use, disclosure or request. The HITECH Act requires HHS to issue guidance on what constitutes "minimum necessary." In the NPRM, HHS solicits public comment on what aspects of the minimum necessary standard should be addressed in the guidance.

Expansion of Individuals' Rights to Restrict Disclosure of PHI to Health Plans

The NPRM proposes a new exception to the general rule that a covered entity is not required to accede to an individual's request that the covered entity restrict disclosure of its PHI. Specifically, HHS would require a covered entity, upon request from an individual, to agree to a restriction on the disclosure of PHI to a health plan if: (1) the disclosure is for the purposes of carrying out payment or healthcare operations and is not otherwise required by law; and (2) the PHI pertains solely to a health care item or service for which the individual,

or person on behalf of the individual other than the health plan, has paid the covered entity in full. Covered entities would be required to notify individuals of their ability to request such a restriction in the Notice of Privacy Practices. HHS recognizes that this restriction may be difficult to implement in situations where multiple entities are involved in an individual's care, and requests comment on how to address this issue. Specifically, HHS requests suggestions for methods through which a provider, using an automated electronic prescribing tool, could alert pharmacies that individuals have requested that a restriction be placed on the disclosure of their PHI to a health plan and that the individuals intend to pay for the prescription out of pocket.

In addition, the NPRM makes clear that, when an individual requests a restriction of PHI to a health plan and pays out of pocket for the treatment or service, the payment would not count towards the individual's out of pocket threshold with respect to his or her health plan benefits. HHS requests comment on how this would impact HMOs, which do not require payments for individual treatments, and as such, may require HMO members to use an out-of-network provider to comply with the provision. The NPRM also notes that, if an out of pocket payment is not honored, the provider is permitted to submit a claim to the health plan for payment, despite an individual's request for a restriction. Further, if an individual terminates a previously-requested restriction, HHS recognizes that a provider may need to submit information regarding those prior treatments to a health plan in order to request payment for follow-up treatments.

Expansion of Individuals' Rights of Access to PHI

The HITECH Act expands an individual's right to review or obtain copies of his or her PHI maintained

in electronic health records. To maintain consistency in the HIPAA Rules, the NPRM implements these new requirements with regard to an individual's right to access PHI maintained in any format, including electronic PHI. The NPRM proposes that, if PHI requested by an individual is maintained electronically in one or more designated record sets, a covered entity must provide the individual with access to the electronic information in the electronic form and format as agreed to by the covered entity and the individual, if readily producible.

The NPRM also proposes to require a covered entity to transmit a copy of PHI directly to another person designated by the individual, if so requested by the individual. In addition, the covered entity may not charge more than its labor costs in responding to a request for access to PHI (which should be negligible in the case of electronic copies), although if an individual requests that the electronic copy be provided on portable media, the NPRM proposes to allow the covered entity to charge a reasonable cost-based fee for the cost of supplies for creating the paper copy or electronic media (*e.g.*, CD or flash drive). HHS also requests comment on the appropriate time limits for the provision of access to PHI by covered entities.

In addition to notifications regarding communications for treatment purposes, fundraising and the right to restrict disclosures to health plans described above, the NPRM proposes that the Notice of Privacy Practices should include a statement that describes all of the uses and disclosures of PHI that require an individual authorization. HHS also requests comment regarding whether the Notice of Privacy Practices (and the HIPAA Privacy Rule itself) should contain specific information regarding HITECH's requirement that affected individuals, the media and the Secretary of HHS be notified following a breach of unsecured protected health

information. In addition, HHS requests comment on whether the requirement that health plans revise and redistribute the Notice of Privacy Practices within 60 days of material changes therein should be modified.

* * *

Latham & Watkins LLP has considerable experience with advocacy regarding legislative and regulatory developments, as well as counseling organizations on the adoption of HIPAA compliance programs. Please feel free to contact the authors if you would like assistance with submitting comments on this NPRM or if you have any questions regarding the proposed changes to the HIPAA regulations.

If you have any questions about this *Client Alert*, please contact one of the authors listed below or the Latham attorney with whom you normally consult:

W. Andrew H. Gantt III
+1.202.637.2259
andrew.gantt@lw.com
Washington, D.C.

Preeya M. Noronha
+1.202.637.1083
preeya.noronha@lw.com
Washington, D.C.

Client Alert is published by Latham & Watkins as a news reporting service to clients and other friends. The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the attorney with whom you normally consult. A complete list of our *Client Alerts* can be found on our website at www.lw.com.

If you wish to update your contact details or customize the information you receive from Latham & Watkins, please visit www.lw.com/LathamMail.aspx to subscribe to our global client mailings program.

Abu Dhabi	Houston	Paris
Barcelona	London	Riyadh*
Beijing	Los Angeles	Rome
Brussels	Madrid	San Diego
Chicago	Milan	San Francisco
Doha	Moscow	Shanghai
Dubai	Munich	Silicon Valley
Frankfurt	New Jersey	Singapore
Hamburg	New York	Tokyo
Hong Kong	Orange County	Washington, D.C.

* In association with the Law Office of Mohammed A. Al-Sheikh