SHIPMAN & GOODWIN LLP®
COUNSELORS AT LAW

Health Law

AUGUST 2010

HHS Announces Proposed HIPAA Rules

On July 8, 2010, the Department of Health and Human Services ("HHS") proposed modifications to certain provisions of the Health Information Technology for Economic and Clinical Health Act ("HITECH") and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (the "Proposed Rule"). The Proposed Rule is not final and does not change current law or regulations, unless and until a final rule is issued. Covered entities, business associates and other interested parties can submit comments on the Proposed Rule to HHS no later than September 13, 2010. The following summarizes some of the key changes addressed by the Proposed Rule.

I. Business Associates.

Subcontractors. The Proposed Rule would expand the definition of business associate to include "subcontractors" (other than workforce members) that create, receive, maintain, or transmit PHI on behalf of a business associate. HIPAA would apply to all downstream subcontractors in the same manner as it applies to business associates that directly contract with or act on behalf of covered entities, and subcontractors would incur the same liability for noncompliance. Subcontractors must enter into business associate agreements with the business associate or upstream subcontractor that engaged the subcontractor. The Proposed Rule also clarifies that covered entities are liable for the acts of business associates and business associates are liable for the acts of subcontractors when the business associate or subcontractor is an agent.

Data Transmission Entities/Vendors of Personal Health Records. In accordance with HITECH, entities that provide data transmission services to a covered entity involving protected health information ("PHI") and that require routine access to such PHI are business associates. Such entities include, but are not limited to, Health Information Exchange Organizations, Regional Health Information Organizations and E-Prescribing Gateways. Under the Proposed Rule, such entities are more generally referred to as "Health Information Organizations." In addition, an entity that manages the exchange of PHI through a network, whether through a patient locator service or by providing oversight or governance functions for the exchange, would be a business associate.

The Proposed Rule also provides that a vendor that contracts with a covered entity to offer a personal health record to patients as part of the covered entity's electronic health record would be a business associate.

Patient Safety Organizations ("PSO"). The Patient Safety and Quality Improvement Act provides that a PSO is a business associate of the covered entity for which it provides a service. The Proposed Rule incorporates this concept into HIPAA by adding patient safety activities to the list of functions and activities that may be undertaken on behalf of a covered entity by a business associate.

Health Law Practice Group:

Joan W. Feldman
(860) 251-5104
jfeldman@goodwin.com

David M. Mack
(860) 251-5058
dmack@goodwin.com

John H. Lawrence, Jr.
(860) 251-5139
jlawrence@goodwin.com

Vincenzo Carannante
(860) 251-5096
vcarannante@goodwin.com

Lina Estrada McKinney
(860) 251-5660
lmckinney@goodwin.com

William J. Roberts
(860) 251-5051
wroberts@goodwin.com

Business Associate Agreements. The Proposed Rule requires that the business associate agreement include language with respect to:

- Ensuring subcontractors implement reasonable and appropriate safeguards to protect the security of electronic PHI ("ePHI");
- The business associate's obligation to report to the covered entity breaches of unsecured PHI and security incidents;
- Ensuring that business associates comply, where applicable, with HIPAA's security rule with regard to ePHI; and
- Ensuring that any subcontractors that create or receive PHI on behalf of a business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information.

In addition, HHS proposes to eliminate the requirement that a covered entity report to HHS when (i) it knows of a pattern or practice of the business associate that amounts to a material violation of the business associate agreement, (ii) the business associate fails to cure the breach and (iii) termination of the business associate agreement is not feasible.

HHS may permit covered entities and business associates to continue to operate under their existing business associate agreements for up to one year after the Proposed Rule's compliance date (180 days after the effective date of the final rule). This transition period would be available to a covered entity or business associate if, prior to the publication of the final rule, the covered entity or business associate had an existing compliant business associate agreement that was not renewed or modified between the final rule's effective date and 180 days thereafter.

II. The Enforcement Rule.

As discussed more fully in Shipman & Goodwin's December 8, 2009 client alert on this topic, HITECH and its October 30, 2009 interim final rule significantly modified HHS' enforcement of HIPAA regulations and application of penalties. The Proposed Rule clarifies some outstanding issues from the interim final rule and provides further guidance.

Complaints and Investigations. Currently, HHS has discretion to investigate complaints and to resolve noncompliance by informal means. Under the Proposed Rule, where a preliminary review of the facts indicates a possible violation due to willful neglect, HHS would be required to conduct a compliance review and investigate any complaints. If a violation due to willful neglect is uncovered, HHS is required to impose a civil monetary penalty.

Civil Monetary Penalties. HITECH established four tiers of penalties based upon increasing levels of culpability applicable to HIPAA violations by covered entities or business associates occurring on or after February 18, 2009. The Proposed Rule clarifies how HHS will determine under which tier a violation fits, and how a penalty amount within the tier's permissible range will be determined. The Proposed Rule modifies the four tiers as follows:

- Lack of Knowledge and Reasonable Diligence. The lowest penalty tier applies when a covered entity or business associate did not know (and by exercising reasonable diligence would not have known) of a violation. Please note, however, that under the Proposed

Rule knowledge of a workforce member may be imputed to the covered entity or business associate, so that if an employee knew or could have known of a violation the covered entity or business associate would not be eligible for this tier.

- Reasonable Cause. The reasonable cause tier applies when a covered entity or business associate, despite the exercise of ordinary care and prudence, failed to comply with HIPAA as a result of reasonable causes or circumstances. Under this tier, a covered entity or business associate could not have consciously or intentionally failed to comply or recklessly disregarded its obligations to comply.

- Willful Neglect. The highest two tiers are for violations due to willful neglect. Willful neglect requires the conscious, intentional failure or reckless indifference to comply (e.g. failure to implement policies and procedures, refusal to comply or failure to respond). If a violation due to willful neglect is timely corrected, HHS will treat the violation as less severe than if not timely corrected. The Proposed Rule indicates that HHS will use a "broad" interpretation of whether or not a violation is corrected, which may include remedying the harm or revising the noncompliant policies or procedures that contributed to the violation.

Within each tier, HHS has the discretion to set the specific penalty amount. When making this determination, HHS will now consider the nature and extent of the violation (e.g. time period, number of individuals affected by the violation), the nature and extent of the harm (e.g. physical, financial or reputational) resulting from the violation and the entity's HIPAA compliance history. Penalty amounts have not changed as a result of the Proposed Rule. Please see the below table for penalty ranges:

Type of Violation	Range for Each Violation	Maximum Aggregate Penalty per Calendar Year for Each Violation
Lack of Knowledge	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 - $50,000	$1,500,000
Willful Neglect – Corrected	$10,000 - $50,000	$1,500,000
Willful Neglect – Not Corrected	$50,000 (minimum)	$1,500,000

III. The Privacy Rule.

Marketing. HIPAA requires a covered entity to obtain a patient's authorization before using or disclosing a patient's PHI for marketing purposes. Marketing is any communication that encourages an individual to purchase a good or service. Marketing does not include face-to-face communications, promotional gifts of nominal value or health education communications that do not promote a specific product or service. HHS proposes that the following types of communications would also not be considered marketing:

- Certain "health care operation" communications, unless the covered entity receives "financial remuneration" in exchange for making the communication. The exception includes communications discussing (i) health care related services offered by the covered entity, and (ii) care coordination, case management, and notice of treatment alternatives

targeted at a certain population (e.g. the covered entity's cancer patients). "Financial remuneration" is direct or indirect payment from or on behalf of a third party whose product or service is being described. Financial remuneration does not include payment for treatment of an individual or any type of non-monetary remuneration.

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

- Treatment communications targeted at specific individuals (as opposed to a population as described in the first exception above), such as care coordination and contacting individuals about treatment alternatives. If the communication is in writing and financial remuneration is received in exchange for making the communication, the covered entity must include a statement in its notice of privacy practices informing individuals that the provider may send subsidized communications to the individual concerning treatment alternatives or other health-related products or services, and the individual has a right to opt out of receiving the communication. Moreover, the treatment communication itself must disclose that financial remuneration was provided and offer the opportunity to opt out of receiving future communications. The method of opting out may not cause undue burden and cannot require a written request to opt out.

Sale of Protected Health Information. HITECH prohibits a covered entity or business associate from receiving remuneration in exchange for the disclosure of PHI unless an exception applies or the covered entity has obtained a valid authorization. A covered entity may receive remuneration in exchange for the disclosure of PHI when the purpose of such disclosure is for public health activities, research, treatment of an individual, certain health care operations, activities undertaken by a business associate on behalf of a covered entity, or the exchange is to provide an individual with a copy of his or her PHI.

In implementing this requirement, the Proposed Rule would require the authorization to state that the covered entity will receive remuneration for the disclosure or sale of PHI to a third party. The Proposed Rule also clarifies that a separate authorization would be required for each disclosure, in that, if a covered entity sells PHI to a business associate pursuant to an authorization, the business associate would need a separate authorization to further sell the PHI.

Research. HHS proposes to allow a covered entity to combine conditioned and unconditioned authorizations for research, provided that the authorization clearly differentiates between the conditioned and unconditioned research components and allows the individual to opt in to the unconditioned research activities. For example, HHS proposes to allow a covered entity to combine an authorization permitting the use and disclosure of PHI associated with a specimen collection for a central repository and an authorization permitting use and disclosure of PHI for clinical research that conditions research-related treatment on the execution of a HIPAA authorization.

PHI About Decedents. Currently, a covered entity may only disclose a decedent's PHI with authorization from the individual's personal representative. In response to the difficulties of disclosing a deceased person's PHI due to locating personal representatives, HHS proposes that individually identifiable health information of a person who has been deceased for more than 50 years is not PHI and would therefore not be subject to HIPAA's privacy and security protections.

In addition, the Proposed Rule would permit covered entities to disclose a decedent's PHI 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 to any known prior expressed preference of the individual.

Disclosure of Student Immunizations to Schools. Due to concerns that HIPAA may inadvertently prevent students from attending school by making it difficult for parents to provide necessary immunization records to schools, HHS proposes to permit covered entities to disclose proof of immunization to schools in states that require students to be immunized prior to school attendance. Instead of requiring a written authorization to disclose such information, the covered entity would be required to obtain oral or written consent.

Minimum Necessary. HIPAA requires that disclosures of PHI be limited to the minimum necessary to achieve the intended purpose. HITECH provides that a covered entity shall be treated as complying with HIPAA's minimum necessary standard only if it limits PHI, to the extent practicable, to the limited data set. HHS is requesting comment on what aspects of the minimum necessary standard HHS should address.

Fundraising. HIPAA presently requires a covered entity to describe how to opt out of receiving future fundraising communications in fundraising materials. HHS proposes to strengthen this provision by requiring the covered entity to provide a clear and conspicuous opportunity in the communication for the individual to elect not to receive any future fundraising communications. To satisfy this requirement, the method to elect not to receive future communications may not cause the individual to incur any undue burden or more than nominal cost. For example, a toll-free number or email address would be acceptable, while requiring the individual to write and mail a letter to the covered entity would not. Moreover, a covered entity may not condition treatment or payment on an individual's decision to opt out.

Notice of Privacy Practices. The Proposed Rule proposes that a covered entity's notice of privacy practices will be required to include:

- A statement that describes certain uses and disclosures of PHI that require an authorization and that other uses and disclosures not described in the notice will be made only with the individual's authorization.
- Notice that most uses and disclosures of psychotherapy notes and those for marketing purposes require an authorization.
- If applicable, notice that the individual has the opportunity to opt out of receiving communications about treatment alternatives or health-related products or services when the provider receives financial remuneration for such services.
- If applicable, a statement to inform individuals that they may be contacted to raise funds for the entity and that they have the right to opt out of such communications.
- A statement that the covered entity must agree to certain requests for restrictions, as discussed below.

HHS has requested comments regarding whether the notice of privacy practices should address the covered entity's obligation to notify individuals, the media or HHS following a breach of unsecured PHI.

IV. Individual Rights.

Requesting Restrictions. The Proposed Rule implements HITECH to require a covered entity, upon request from an individual, to agree to a restriction on the disclosure of PHI to a health plan if (i) the disclosure is for the purposes of carrying out payment or health care operations and is not otherwise required by law, and (ii) the PHI pertains solely to a health care item or service for which the individual has paid the covered entity in full. The Proposed Rule also makes clear that this provision applies when another person pays in full on behalf of the individual.

The Proposed Rule would prohibit a provider from requiring a patient to pay for all care of out-of-pocket in order to have the restriction for certain care. The Proposed Rule requests comments on how this restriction would be applied in certain circumstances, such as through an E-Prescribing Gateway or to downstream providers. The Proposed Rule also would permit a provider to bill a payer if the out-of-pocket payment is not honored (e.g. a bounced check) and the covered entity is unable to resolve the payment issue.

Access and Transmission of PHI. Pursuant to HITECH, when a covered entity maintains an individual's ePHI in one or more designated record sets, the individual has a right to obtain a copy of that ePHI in an electronic format requested by the individual if it is readily producible, or if not, in a readable electronic format agreed to, and may direct the covered entity to transmit the ePHI to a third party. The Proposed Rule would expand the scope of the provision to require the covered entity to transmit, upon request, a copy of any PHI of the individual it maintains, without regard to whether the PHI is in electronic or paper format, and to verify the identity of the individual requesting the transmission.

V. Concluding Comments.

The Proposed Rule is not final law and is HHS' proposal on how to apply certain HITECH provisions and introduce other changes to the HIPAA regulations. Providers and business associates should be aware of their potential future obligations as they consider their HIPAA compliance programs and may provide comments to HHS on areas of interest or on reform generally.

Questions or Assistance? If you have any further questions regarding HIPAA compliance, please feel free to contact either any of the following members of our Health Law Practice Group:

Joan W. Feldman
(860) 251-5104
jfeldman@goodwin.com

David M. Mack
(860) 251-5058
dmack@goodwin.com

John H. Lawrence, Jr.
(860) 251-5139
jlawrence@goodwin.com

Vincenzo Carannante
(860) 251-5096
vcarannante@goodwin.com

Lina Estrada McKinney
(860) 251-5660
lmckinney@goodwin.com

William J. Roberts
(860) 251-5051
wroberts@goodwin.com

One Constitution Plaza
Hartford, CT 06103-1919
860-251-5000

300 Atlantic Street
Stamford, CT 06901-3522
203-324-8100

1133 Connecticut Avenue NW
Washington, DC 20036-4305
202-469-7750

289 Greenwich Avenue
Greenwich, CT 06830-6595
203-869-5600

12 Porter Street
Lakeville, CT 06039-1809
860-435-2539

www.shipmangoodwin.com

www.shipmangoodwin.com

SHIPMAN & GOODWIN LLP®
COUNSELORS AT LAW