HUNTON& WILLIAMS

CLIENT ALERT

August 2009

Contacts

Dallas Office
1445 Ross Avenue, Suite 3700
Dallas, Texas 75202-2799
(214) 979-3000

L. Scott Austin**
saustin@hunton.com

Baker R. Rector
brector@hunton.com

Henry Talavera
htalavera@hunton.com

James A. Deets
jdeets@hunton.com

McLean Office
1751 Pinnacle Drive, Suite 1700
McLean, Virginia 22102
(703) 714-7400

David A. Mustone
dmustone@hunton.com

Christina M. Crockett
ccrockett@hunton.com

New York Office
200 Park Avenue
New York, New York 10166-0091
(212) 309-1000

John T. Konther
jkonther@hunton.com

Leslie A. Okinaka
lokinaka@hunton.com

Leslie S. Hansen
lhansen@hunton.com

Richmond Office
951 East Byrd Street
Richmond, Virginia 23219-4074
(804) 788-8200

Mark S. Dray
mdray@hunton.com

J.G. Ritter
jritter@hunton.com

**Alternate location for L. Scott Austin:
Atlanta Office
600 Peachtree Street, NE
Suite 4100
Atlanta, Georgia 30308-2216

Upcoming HIPAA Privacy and Security Rule Changes for Group Health Plans

This past February, Congress strengthened (in the American Recovery and Reinvestment Act of 2009) the safeguards for protected health information ("PHI") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). These changes include:

- expanded individual rights concerning the disclosure of PHI, *including* a new notice requirement for the unauthorized use, access or disclosure of PHI (called a "breach");
- the application of the privacy and security rules directly to business associates; and
- increased penalties and enforcement for privacy and security rule violations.

New Privacy Rule Breach Notification Requirements (Effective 9/23/2009)

The new law generally requires covered entities (such as self-insured group health plans) to notify affected individuals of a breach of their "*unsecured*" PHI in any form (electronic, paper or verbal) within 60 days of discovering the breach. Notification of breaches must also be provided to the Department of Health and Human Services ("HHS") as follows: immediately for any breach involving 500 or more individuals, and annually for all other breaches. In addition, recently issued HHS regulations provide that where the breach involves more than 500 individuals in a particular state, prominent media outlets in that state also must be notified within 60 days. To facilitate compliance with these requirements, the new law obligates business associates to notify the covered entity of any such breach within a 60-day timeframe.

In general, PHI is "unsecured" if it is not secured by use of a technology or methodology (approved by HHS) that makes the PHI unusable, unreadable or indecipherable. HHS has issued guidance that generally provides the following methods for securing PHI:

- encryption of electronic PHI (that meets certain standards),
- destruction of hard copies by shredding or otherwise (so that the records are not readable and cannot be reconstructed), and
- destruction or sanitizing of electronic media consistent with certain guidelines.

In addition, recently issued HHS regulations provide that the notice requirement does not apply where the breach *does not pose a significant risk* of financial, reputational or other harm to the affected

individual(s). Nor does it apply to (i) inadvertent disclosures between (and unintentional access by) authorized individuals in the same organization when further use or disclosure complies with the privacy rules, or (ii) "limited data set" disclosures that do not include ZIP Codes and birth dates.

In general, the required notice must be provided in writing, but other means are permitted if the entity has insufficient contact information for affected individuals. The notice must, among other things, briefly describe

- what happened,
- the breached PHI, and
- the steps that the affected individuals can take to protect themselves.

The new notification requirements will go into effect for breaches discovered on or after *September 23, 2009*. Covered plans should consider discussing with their business associates beforehand how any breaches will be handled and who will prepare/issue any required notices. Note also that the HHS regulations provide that a covered entity's privacy policies and procedures must be updated to comply with the notice requirements. Therefore, steps will need to be taken in this regard as well.

Extension of Privacy/Security Rules to Business Associates (Effective 2/17/2010)

As originally enacted, the HIPAA privacy and security rules applied only to covered entities — generally, health plans, health care providers and health care clearinghouses. Because business associates are not covered entities, they are only contractually obligated to follow the HIPAA safeguards as provided in their business associate agreement. The new law changes this, since it provides that, beginning February 17, 2010, business associates must adhere to the same administrative, physical and technical safeguards that apply to covered entities. This change will require amendments to be made to existing business associate agreements by that deadline. In the meantime, covered entities should obtain assurances from their business associates that they will be ready to comply with their new HIPAA obligations at that time.

New Disclosure Rules

As mentioned above, the new law also makes some changes to the privacy disclosure rules, which are briefly described below. Note that it will be necessary to incorporate these changes in a timely manner into the covered entity's HIPAA privacy notice and policies (as applicable).

1. *Access to Certain Electronic PHI (Effective 2/17/2010)*. Under current law, individuals have the right to obtain a copy of their PHI from a covered entity, which may charge the copying, postage and labor costs for producing these records. The new law expands this right by providing that an individual must also have the right to obtain "electronic health records" maintained by the covered entity (or have them sent to a designated third party). The covered entity may charge only the labor costs for retrieving these records. For this purpose, "electronic health records" include only health-related information collected for health care clinicians and staff — information that is typically held by business associates, and not by health plans themselves. Therefore, it will be important to sort out with business associates (where applicable) to what extent they will be responsible for handling such disclosure requests on a plan's behalf.

2. *Individual Right to Restrict Certain Disclosures (Effective 2/17/2010)*. Covered entities have the discretion (but are not obligated) under current HIPAA rules to restrict the disclosure of an individual's PHI upon request. This will change in minor respects under the new law. Anyone who pays th++)e full cost of a health provider's care will be able to require that any PHI related to that care not be disclosed to a health plan for payment or health care operations. However, this limit will not apply to any disclosures that are necessary for medical care.

3. *Limited Disclosure (Effective 8/17/2010)*. The current HIPAA rules generally provide that permitted disclosures of PHI must be limited to the "minimum necessary" to accomplish the purpose for which disclosure is being made. The new law provides that only "limited data set" information should be disclosed unless more is needed, in which case disclosure can be made in accordance with the "minimum necessary" rule. At the same time, the new law also requires HHS to reexamine the scope/application

of the "minimum necessary" rule and issue guidance by August 1, 2010.

4. *Limits on Marketing Communications (Effective 2/17/2010)*. Under current law, marketing communications generally are not permitted unless individual authorization is given or the communication is made in connection with the "health care operations" of the covered entity. To qualify for the health care operations exception under the new law, the covered entity may not (with some exceptions) receive any compensation for the communication. The new law also generally prohibits the payment of remuneration for the exchange of PHI. However, this does not apply where the exchange is for public health activities, research, services provided pursuant to a business associate contract or other purposes permitted under HHS regulations.

5. *PHI Disclosure Accounting (effective 1/1/2011 for PHI acquired after 2008 and 1/1/2014 for PHI acquired before 2009)*. Under current law, individuals are entitled to request an accounting of PHI disclosures (other than those made for payment, treatment or health care operations ["PTO"] and certain other purposes) for the previous six years. The new law extends this right to PTO disclosures of "electronic health information" (defined above) made during the previous three years.

Enhanced Penalties and Enforcement (effective 2/17/2010)

Increased penalties for noncompliance will go into effect on February 17, 2010, and will, for the first time, apply to business associates. The new law provides for tiered penalties ranging from $100 to $50,000 per violation (with annual caps per violation type), the application of which will turn on the nature and extent of the violation and culpability. For example, persons who lack knowledge, and would not have known of the violation after exercising due diligence, are subject to the lowest tier of penalties. The new penalties generally will not (as under current law) apply to violations corrected within 30 days.

The new law also requires that HHS conduct periodic audits to ensure that both covered entities and business associates are in compliance with their HIPAA privacy and security obligations. In addition, state attorneys general also will have the authority to bring civil actions against covered entities for privacy and security rule violations to enjoin violations or recover damages (up to certain limits) for the state's residents.

We welcome the opportunity to answer any questions you may have regarding the new HIPAA rules or to assist you in assessing your options for complying with those rules.