MILLER CANFIELD

New HIPAA Rule for Group Health Plans and Health Care Providers

Requires Notification of Breach of Unsecured Protected Health Information

September 16, 2009

The first of many amendments to HIPAA under the Health Information Technology for Economic and Clinical Health Act (HITECH) takes effect on September 23, 2009. Until now, HIPAA did not require covered entities to notify individuals of breaches of their protected health information, unless the individuals specifically requested an accounting of unauthorized disclosures. Subject to certain exceptions, covered entities such as health plans and health care providers must now give notice to affected individuals of a breach of unsecured protected health information. In some cases, the required notice will include alerting the news media as well as individual mailings.

As might be expected with anything HIPAA-related, the rules are complicated:

- A "breach" occurs when there is unauthorized acquisition, access, use or disclosure of protected health information that poses a significant risk of financial, reputational, or other harm to an individual.
- Protected health information (PHI) is "unsecured" unless it is rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Department of Health and Human Services (HHS). According to HHS guidance, electronic PHI is "secure" only when it is encrypted, and hard copy PHI (such as documents and film media) is secure only when destroyed in such a manner that it cannot be read or reconstructed.

The required notice will vary depending on the scope of the breach. In all cases, notice must be given "without unreasonable delay" and in no case later than 60 days after discovery of the breach. Discovery is presumed if any employee (other than the person who committee the breach) knows or should know that the breach occurred. The notice must be written in plain language and must disclose:

- when the breach was discovered
- how and when the breach occurred
- the types of unsecured protected health information involved
- the steps individuals should take to protect themselves from harm
- what the covered entity is doing to investigate the breach, mitigate harm, and protect against further breaches.

In all cases, the covered entity must notify affected individuals in writing by U.S. mail or e-mail. If the breach affects more than 500 residents in a particular state or jurisdiction, however, the covered entity must also notify prominent media outlets. The covered entity must report breaches to HHS on an annual basis, but in the case of a breach affecting more than 500 individuals (regardless of location), the covered entity must notify HHS at the same time that it notifies the affected individuals. A HIPAA business associate that discovers a breach of unsecured PHI is required to give notice to the covered entity so that the covered entity may give the required notice to affected individuals.

Continued

The breach notification rule is just one of many changes made by HITECH. Other amendments, slated to go into effect starting in February 2010:

- require business associates to comply with most provisions of the HIPAA Security Rule and Privacy Rule
- strengthen individuals' rights to designate restrictions on disclosures of their PHI
- provide a right of access to electronic PHI
- modify the circumstances under which "marketing" communications must be authorized by individuals
- provide that HIPAA's criminal penalties can be enforced against individuals, including employees of covered entities
- clarify when civil money penalties can be pursued