crowell moring

CLIENT ALERT

Updates on the HIPAA Breach Notification Requirements

Oct.15.2009

On October 1, 2009, the US House Ways and Means Committee and the House Energy and Commerce Committee sent a joint letter to the Secretary of Health and Human Service urging her to "revise or repeal" the recent guidance offered by HHS in its interim final rule which included a harm standard for breach notification. If the guidance stands, Covered Entities and their Business Associates will not be required to notify affected individuals of a breach involving their PHI unless there is a "significant risk of financial, reputational or other harm to the individual." According to HHS, the risk of harm standard would allow CE's and BA's to forego notification in circumstances such as an inadvertent disclosure to another CE, or a disclosure that was immediately remedied. In the October letter, the Committee members explain that they specifically considered including a harm standard in the breach notification statute and rejected it (as have many states and other House and Senate committees considering a general breach notification law).

According to the letter, the intent of the Committee members was to develop a "black and white standard for notification with a safe harbor for information that is rendered unusable, unreadable, or indecipherable to unauthorized individuals, and other specific exceptions." The purpose of this "black and white standard" was to provide incentives for CE's and BA's to protect PHI through strong encryption or destruction methodologies and to promote transparency with the consumer. It is unclear at this junction what effect this letter will have on HHS. However, it is quite clear that if the harm standard is eliminated, each and every unauthorized acquisition, access, use or disclosure of PHI will be subject to the current notification requirements, and it will be left to the affected individuals to decide what level of harm exists, and thus what level of remediation is warranted.

In a less controversial vein, but perhaps equally confusing, HHS released its proposed forms for reporting breaches. While the forms themselves are relatively straightforward, the process for submitting them is not. In the August interim final rule issued by HHS, the process for breaches involving less than 500 individuals was to "log" the breach and submit the log in an annual report no later than 60 days following the end of the calendar year. However, the forms provide only for immediate electronic submission. Therefore, it appears that CE's and BA's will be forced to either submit these electronic forms as breaches occur, or document each incident in the same level of detail and submit multiple forms within the designated timeframe at the end of each year. Also, the forms do not seem to be intended for breaches where notification is not sent because the risk of harm was low or nonexistent. The ambiguity lies in the process, but for now, it appears that these breaches will be documented internally along with the detailed risk of harm assessment.

Click here to access the OCR forms.

If you would like to learn more about the HIPAA breach notification requirements, or would like assistance updating your policies, procedures, training or with sample language, please contact those listed below or your regular Crowell & Moring contact.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Barbara H. Ryland
Senior Counsel – Washington, D.C.
Phone: +1 202.624.2970
Email: bryland@crowell.com