Paul Hastings
Stay Current
A Client Alert from Paul Hastings
August 2009

Obligations Imposed by Stimulus in Cases of Breach Involving Protected Health Information Clarified

BY ERIC KELLER AND KELLY DEMARCHIS

As we reported in a March 2009 Paul Hastings Stay *Current*,[1] the fiscal stimulus package (the "Act") included large-scale expansion of the health information privacy and security provisions that are part of the Health Insurance Portability and Accountability Act of 1996 ("HIPPA"). The specifics of these provisions have remained uncertain, pending further rulemaking and guidance from Health and Human Services ("HHS"). On August 19, 2009, HHS issued an interim health information breach notification rule that fills in some of the gaps in the Act. The interim final rule is effective September 23, 2009 and comments regarding the interim final rule may be submitted to HHS on or before October 23, 2009.

The Act adds a notification requirement that applies to HIPAA's "covered entities" and their "business associates" (generally defined as entities that provide services such as claims processing, data analysis, and billing to covered entities). It requires that they notify individuals of a breach of their "unsecured protected health information ('PHI')" within 60 days of discovery of the breach. According to the Act, covered entities are deemed to have knowledge of a breach if they "should reasonably have known" of the breach. Notification must be written and sent by first-class mail to the individual's last known address, or notice can be via electronic mail if the individual previously specified a preference for electronic notice. If there is insufficient or out-of-date contact information, covered entities may substitute conspicuous posting on its webpage or notice in major print or broadcast media. Substitute notice must include a toll-free phone number that an individual can call to verify if his or her PHI was affected.

HHS's August interim rule further explains what covered entities and business associates are required to do in order to provide sufficient notice in the case of a security breach that affects PHI.

When Notice is Required

HHS's interim rule states, generally, that a covered entity shall, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been accessed, acquired, used, or disclosed as a result of such breach. "Breach" is defined as the acquisition, access, use, or disclosure of PHI in an unpermitted manner, and which compromises the security or privacy of the PHI by posing a significant risk of financial, reputational or other harm to the individual who is the subject of the PHI.

A breach is "discovered" by a covered entity either on the first day on which the breach is known to the covered entity, or when it would have been known if the covered entity had exercised reasonable diligence. Reading both definitions together, the notification obligation is triggered on the day that the unauthorized access, acquisition, use, or disclosure of unsecured PHI is discovered, provided that the breach is believed to compromise the security or privacy of the PHI. The actual notice is required to be delivered within 60 days after the obligation is triggered.

There is one important exception to the notification requirement. Notification is only required for "unsecured" PHI. PHI is unsecured if it is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology specified by HHS. PHI that is properly secured does not require notification in case of a breach. HHS published technical guidance on this point in April 2009 that set forth encryption and other security specifications for electronic PHI.

Contents of the Notice

The Rule also sets forth greater detail about the contents of the notice. It must contain the following elements:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of unsecured PHI that were involved in the breach, such as whether full name, social security number, date of birth, address, etc. were involved;
- Any steps that individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to the individuals, and to protect against further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, website, or postal address.

As mentioned above, notice must be by first-class mail to the last known address of the individual, or via email if the individual has previously agreed to receiving notice this way. There are also substitute notice provisions in cases where there is insufficient or out-of-date contact information, and notice must also be provided through the media if the breach involves more than 500 individuals. In those large cases, notice must also be furnished to HHS contemporaneously with the notice furnished to the affected individuals. If the breach involves less than 500 individuals, notice must be furnished to HHS no later than 60 days after the calendar year in which the breach occurred in the manner specified on HHS's website.

Parallel Rulemaking from the Federal Trade Commission

The Federal Trade Commission ("FTC") issued parallel rulemaking in conjunction with HHS. The FTC's rule only applies to businesses or organizations that maintain personal health records but are not covered by HIPAA, and to information that is not secured through technologies specified by HHS. An example might include a business that has a website that allows people to maintain their medical information online.

The breach notification procedure and requirements mirror those promulgated by HHS. The FTC has created a standard form for reporting breaches to the agency. This form is available on the FTC website at http://www.ftc.gov/os/2009/08/R911002hbnform.pdf.

The FTC rule has already gone through the comment period and enforcement will begin in approximately 210 days.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings Washington D.C. lawyers:

Eric R. Keller
202-551-1770
erickeller@paulhastings.com

Kelly A. DeMarchis
202-551-1828
kellydemarchis@paulhastings.com

[1] Paul Hastings, *Stronger Protections for Health Information are Part of the Fiscal Stimulus* (Mar. 17, 2009), *available* by following this link.