Compliance Alert

FEATURED ATTORNEY

Patrick Formato
Executive Partner

On August 19, 2009, the federal Department of Health and Human Services released interim final regulations in connection with the notification of breaches of unsecured protected health information under the privacy and security rules associated with the Health Insurance Portability and Accountability Act of 1996. The final interim regulations were published in the August 24, 2009 Federal Register (74 Fed. Reg. 42,740).

Background

As part of the federal stimulus package passed by Congress last February (the American Recovery and Reinvestment Act of 2009, or “ARRA”, HIPAA received its first major legislative refinement since its initial promulgation in 1996. The Health Information Technology for Economic and Clinical Health (“HITECH”) Act, which comprises part of ARRA, made several noteworthy changes to HIPAA. For the first time, covered entities have an obligation to notify those individuals affected by a breach of “unsecured protected health information” (“UPHI”).

In the April 27, 2009 version of the Federal Register, HHS promulgated “Guidance and Request for Information,” in which HHS defined UPHI and identified HHS-approved technologies that could be used to “secure PHI.” The interim final regulations build on and refine this guidance in response to public comments received by HHS.

Effective Date

The final interim regulations go into effect 30 days after their publication in the Federal Register, making the effective date September 23, 2009. However, HHS acknowledged the short timetable by indicating that it will not impose sanctions for a covered entities failure to comply with the breach notification rules for 180 calendar days after the rules become effective. Instead, HHS will work with covered entities, through technical assistance and voluntary corrective action, to achieve compliance.

What is Considered a Breach?

Generally (although there are exceptions), the new breach notification rules require covered entities to report breaches of UPHI. A breach is any acquisition, access, use or disclosure that is not permitted by HIPAA's privacy rule and which compromises the security or privacy of protected health information ("PHI").

"Compromises the security or privacy of PHI" means to pose a significant risk of financial, reputational or other harm to the individual. Factors that can be used to make this determination include who impermissible used or obtained the information, the type of information involved, whether the covered entity took immediate steps that eliminated or reduced the risk of harm and whether the information was returned prior to being used for an improper purpose. Therefore, upon an unauthorized acquisition, access, use or disclosure of UPHI, a covered entity will have to determine (1) whether it has violated the HIPAA privacy rule, (2) whether that privacy rule violation is likely to pose a significant risk of some harm to the affected individual, and (3) whether any exception applies.

UPHI is any PHI that is not rendered unusable to unauthorized individuals through the use of technology specified in the April 27, 2009 Federal Register guidance mentioned above. Please note that the breach notification rules do not require PHI to be encrypted; the breach notification rules continue HIPAA's flexible compliance approach, nor do they apply to a breach PHI that has been secured using an HHS-approved technology (encryption or destruction of PHI).

What About Business Associates?

Business associates must report breaches to the covered entity with whom they have contracted. It is then the covered entity's responsibility to promptly report the breach to the affected individuals. Remember that, under HITECH, business associates will be directly liable under HIPAA for not reporting breaches to covered entities in accordance with the new breach notification rules.

In What Timeframe Do Breaches Have to be Reported?

Notifications by covered entities and business associates must be made "without unreasonable delay" and in no event later than 60 calendar days after discovery of a breach. The date of the breach will be the date of actual discovery or the date any person (other than the person committing the breach) would have known about the breach through the exercise of "reasonable diligence." The 60 day timeframe is intended as an outer limit only; if a covered entity is in a position to report the breach before the expiration of the 60 days it must do so.

In a somewhat complicated twist, the timeframe for reporting by a covered entity of a business associate's breach depends on the business associate's relationship with the covered entity. If the business associate acts as an agent of the covered entity, the covered entity must report within 60 days (or sooner if it reasonably can) of the business associate's discovery of the breach. In contrast, if the business associate is an independent contractor of the covered entity, then the clock starts upon the business associate's disclosure of the breach to the covered entity.

Who Must be Notified and How?

Affected individuals must be notified by first class mail to their last known addresses or by electronic mail if they have agreed to receive electronic notice. Alternative methods of notification are contemplated in the event the covered entity has outdated contact information for affected individuals. The number of

individuals involved in the notification dictates additional parties that may have to be notified (e.g., “prominent media outlets” must be notified in the event 500 or more individuals are affected).

What Must be in the Notice?

The notice must be written in plain language and include:

- A brief description of what happened, including the date of the breach and the date of its discovery;
- A description of the UPHI involved;
- Any steps individuals should take to prevent themselves from potential harm caused by the breach;
- A description of what the covered entity is doing to investigate the breach, mitigate harm and protect against further breaches; and
- Contact information for follow-up.

What Should You be Doing Now?

The new breach notification rules and certain provisions of the HITECH Act will require covered entities and business associates to revisit their privacy and security policies and, most notably, decide whether they will continue to maintain UPHI or choose to utilize one of the technologies identified by HHS. Business associate agreements will have to be reviewed to ensure timely breach notifications of covered entities and also in light of the other HITECH changes that potentially impact business associate agreements. Training on the new breach notification requirements must be provided by affected organizations to their workforces and that training must be documented.

If you have any questions, need additional information or would like to discuss the development of policies and procedures or amendments to business associate agreements to comply with the HITECH and regulatory requirements, please feel free to contact any of the following Abrams Fensterman attorneys:

Patrick Formato at (516) 328-2300
Betsy R. Malik at (516) 328-2300
Barbara Stegun Phair at (516) 328-2300