Health Law Bulletin

provided by:

MITCHELL • BLACKSTOCK

Mitchell • Blackstock • Barnes • Wagoner • Ivers • Sneddon • PLLC

Notification Rules for HIPAA Breaches Take Effect In September – Part 2

Last week, we discussed the new provisions that take effect September 24 that require covered entities and business associates to notify individuals in certain circumstances if their Protected Health Information (PHI) has been breached. Last week, we dealt with the question of determining whether a reportable breach has occurred. If you complete the analysis and determine that, yes, a reportable breach has occurred, the question then becomes, how and to whom do I send the notification?

The timing of the notice. Notice should be provided "without unreasonable delay" and in no case later than 60 days after discovery of the breach.

The content of the notice. The notice is to be written in plain language and should contain:

- A brief description of what happened, including when the breach was discovered.
- A description of the types of unsecured PHI that were involved in the breach.
- Any steps that individuals should take to protect themselves from potential harm resulting from the breach.
- A description of what the covered entity is doing to investigate the breach, mitigate the harm to individuals, and protect against any further breaches.
- A toll-free contact telephone number, an email address, a web site, or postal address where individuals can ask questions.

The method of notification. Generally, the notice should be by first-class mail. If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative, the notice should be sent to that individual.

If the covered entity knows that its contact information is out-of-date or it doesn't have sufficient contact information to send a written notice, then substitute notice must be used. If the contact information is missing for fewer than ten individuals, then substitute notice by telephone or other means is acceptable. If there is insufficient contact information for ten or more individuals, the covered entity must post the notice on its web page or in major print or broadcast media covering the geographic area where the affected individuals likely reside. The web or newspaper notice must include a toll-free phone number that is active for at least 90 days where an individual can learn whether his unsecured PHI was included in the breach.

Special rule for large breaches. If the breach involves more than 500 residents of a state or jurisdiction, the covered entity must notify prominent media outlets serving the state or jurisdiction.

Notification to the Secretary of HHS. Any breach that covers 500 or more individuals must be reported to the Secretary of HHS at the same time that the public is notified. For all other breaches, the covered entity must maintain a log and report the breaches annually to the Secretary no later than 60 days after the end of the calendar year.

Remember that we said last week that these new regulations take effect thirty days after their publication, which is September 24, 2009. By that time, you should have adopted policies and trained your employees to be on the lookout for breaches and informed them whom to notify if a breach occurs. In recognition of the time required for covered entities to become familiar with these new rules, the Secretary is using her discretion to not impose sanctions for failure to provide notice for six months, or until February 22, 2010. During this time, you should still comply with the regulations, but you will not be subject to sanction if your notification procedures during this six-month period are deficient.

As we noted last week, there are other sections of the HITECH Act for which regulations will be issued in the future. For now, you should be sure that your policies and employee training include these new requirements regarding notification. You may want to consult an attorney to review your policies and procedures for compliance.