March 1 deadline approaching to submit breach reports

James J. Giszczak, Rick L. Hindmand, Dominic A. Paluzzi | Thursday, February 16, 2017

HIPAA covered entities (healthcare providers, health plans and health care clearinghouses) that discovered a breach of Protected Health Information (PHI) in 2016 involving fewer than 500 individuals are required to report those breaches by March 1, 2017.

The HIPAA Breach Notification Rule requires covered entities to notify the affected individuals, the Secretary of the U.S. Department of Health and Human Services (HHS), and in some cases the media of breaches of unsecured PHI. The Rule also requires business associates (generally, contractors or vendors who perform services or functions for covered entities and have access to PHI) to notify covered entities of breaches of unsecured PHI. Any use or disclosure of unsecured PHI that is not permitted under the HIPAA Privacy Rule is presumed to be a breach and triggers the notification obligations – unless the incident satisfies one of three relatively narrow exceptions or the covered entity or business associate demonstrates a low probability that PHI has been compromised, based on a risk assessment of at least four factors as set forth in the Breach Notification Rule.

Your Notification Obligations

Covered entities must notify affected individuals without unreasonable delay, and in no event more than 60 days after the covered entity discovers the breach (or would have known of the breach if exercising reasonable diligence). The deadline for reporting breaches to the Office for Civil Rights (OCR) depends on whether the breach involves 500 or more individuals. Breaches involving fewer than 500 individuals (sometimes referred to as small breaches) must be reported to OCR no later than 60 days after the calendar year in which the covered entity discovers the breach. Breaches involving 500 or more individuals must be reported to OCR at the same time as the notice to the individuals.

Breaches discovered by a covered entity in 2016 and involving fewer than 500 individuals must be submitted via OCR's website portal by March 1, 2017. The instructions and online Breach Portal are available here. A separate report must be submitted for each breach that occurred during the 2016 calendar year. A copy of the completed form should be printed prior to and after submission and maintained in the covered entity's records to document the notification.

Just last month, OCR announced a $475,000 settlement with Presence Health Network, a Chicago-area health system, for failure to provide timely breach notification to individuals and OCR. OCR's press release and resolution agreement are available here. Moreover, OCR has indicated its intent to step up enforcement arising out of small breaches.

How to properly report a breach

Although the form is available online, it's critical that covered entities and business associates are counseled appropriately through the reporting process to ensure the notification is accurate and consistent with prior messaging regarding the breach. Before completing the online form, it's recommended that organizations

consult with attorneys who have experience in data breach regulatory investigations to avoid any missteps that could come back to harm the organization during an OCR investigation.

For more information, please contact one of the attorneys listed below.

James J. Giszczak

Team member bio

Rick L. Hindmand

Team member bio

Dominic A. Paluzzi

Team member bio