Insights

HHS Issues First Enforcement Action for Failure to Timely Notify Individuals of Breach of PHI

January 9, 2017

By: Stephanie T. Eckerle

On January 9, 2017, the United Stated Department of Health and Human Services, Office of Civil Rights (HHS) announced that it has issued its first enforcement action with a healthcare entity due to the entity's alleged failure to notify affected individuals, HHS and media outlets of a breach of protected health information (PHI) within sixty days. The Resolution Agreement was entered into between HHS and a healthcare entity that operates hospitals, long-term care facilities and physician offices in Illinois according to HHS. The Resolution Agreement between HHS and the healthcare entity stated that on October 22, 2013, the entity discovered that paper operating room schedules were missing that contained PHI of over 800 individuals and that "due to miscommunications between its workforce members, there was a delay in its provision of breach notifications." The individuals were not notified of the breach until February 3, 2014, which was 104 calendar days after discovery of the breach. HHS treated each day after the sixty day reporting period had run as a separate violation of HIPAA's Breach Notification Rule. The entity also failed to notify the media until 106 calendar days after the discovery of the breach and failed to notify HHS until 101 calendar days after notification of the breach. As with the delayed notification to individuals, each day that the healthcare entity failed to notify HHS and the media after the reporting periods lapsed was treated as a separate violation of the Breach Notification Rule. As a result of the healthcare entity's failure to abide by HIPAA's Breach Notification Rule, the entity had to pay $475,000 and enter into a Corrective Action Plan with HHS. The Corrective Action Plan, among other things, requires the healthcare entity to revise its existing policies and procedures, have those policies approved by HHS and provide training on the policies.

It is critical that covered entities and business associates have policies and procedures in place addressing the steps to take when a breach of protected health information is suspected or confirmed. Just as important, the workforce of the covered entity and business associate need to be trained on those policies so that immediate action is taken to investigate a suspected breach, all legal requirements are met under HIPAA and the risk to affected individuals is mitigated. For example, it is important to know that not only must an individual be notified of a "breach" as defined in 45 C.F.R. 164.402 without unreasonable delay and no later than sixty days after the discovery of the breach, but the covered entity must understand when the breach is treated as discovered especially in light of this Resolution Agreement. Pursuant to 45 C.F.R. 164.404, a breach is treated as discovered on the "first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity." The covered entity must also understand how to notify the affected individuals pursuant to the Breach Notification Rule and other guidance from HHS as well as what that notice should contain.

The Resolution Agreement and Corrective Action Plan entered into by HHS and the covered entity demonstrate that HHS takes the Breach Notification Rule very seriously. HHS is sending a clear signal that

covered entities and business associates need to be organized, well-trained and in a position to comply with all aspects of HIPAA, as miscommunications or other administrative mishaps will not justify failure to abide by the Breach Notification Rule. A copy of the Resolution Agreement and Corrective Action Plan can be found here.

Please contact Stephanie T. Eckerle if you have any questions or would like to discuss this matter.