

October 12, 2012

CMS Has HIPAA Breaches Too

On October 10, 2012, the Office of Inspector General (“OIG”) of the Department of Health and Human Services [released a report](#) (“OIG Report”) analyzing the compliance by the Centers for Medicare and Medicaid Services (“CMS”) with the HIPAA notice of breach rules.

CMS is a covered entity under HIPAA and required to comply with HIPAA requirements, including the notice of breach rules. However, the OIG Report found that CMS failed to comply with the requirements of the notice of breach rules in half of the breaches that occurred.

Between September 23, 2009, and December 31, 2011, CMS has reported fourteen breaches of protected health information committed by CMS or its contractors affecting 13,412 individuals. The OIG Report found that CMS failed to comply with the notice of breach rules in seven of those fourteen breaches.

In seven of the breaches, CMS did not notify the individual(s) affected within the required 60-day timeframe, sending notice in one instance more than four months after the 60-day deadline expired. In seven of the breaches, CMS failed to identify in the notice the date the breach occurred or the date the breach was discovered as required by the notice of breach rules. In six of the breaches, CMS did not provide information required in the notice, such as not explaining how the contractors were investigating the breach, mitigating losses, or protecting against further breaches. And in three of the breaches, CMS failed to include other requisite information in the notice, such as the types of unsecured protected health information involved, contact procedures for individuals who want to learn more, or steps individuals can take to protect themselves from harm.

It is easy to see the humor in the fact that even CMS has struggled to comply with the notice of breach rules. But on the serious side, the problems CMS has had identified in the OIG report highlight the need for rapid response to potential breaches, personnel and policies that facilitate a prompt and thorough breach assessment, and diligence in following the proscriptive breach notice requirements.

This E-Mail Alert was prepared by Allen Killworth. Please contact any INCompliance consultant for more information. This and previous E-Mail Alerts may be accessed on our E-Mail Alert webpage.