eALERT

INCompliance

August 22, 2016

OCR announces new initiative to investigate HIPAA breaches affecting fewer than 500 individuals

The Health and Human Services (HHS) Office for Civil Rights (OCR) announced on August 18 that it has launched a new initiative to more widely investigate HIPAA breaches of protected health information (PHI) affecting fewer than 500 individuals. Beginning this month, OCR regional offices have increased their efforts to identify and obtain corrective action to address entity and systemic noncompliance related to these smaller breaches.

OCR has always prioritized its investigation of reported breaches. OCR regional offices are required to investigate all reported breaches involving the PHI of 500 or more individuals, but they have discretion as to whether they will investigate breaches involving the PHI of fewer than 500 individuals. Under this new nationwide initiative, however, the regional offices will investigate more of the smaller breaches, and this will likely result in an increase in corrective actions against covered entities.

The regional offices will maintain their discretion as to which smaller breaches they will investigate. The OCR announcement includes the following five factors that will be considered in determining which breaches to investigate:

- The size of the breach;
- Theft of or improper disposal of unencrypted PHI;
- Breaches that involve unwanted intrusions to IT systems (for example, by hacking);
- The amount, nature and sensitivity of the PHI involved; or
- Instances where numerous breach reports from a particular covered entity or business associate raise similar issues.

The OCR announcement also states that OCR may also investigate covered entities and business associates that may be underreporting breaches. This is the first time OCR has ever stated, in writing, that it would consider the lack of breach reports as the basis for investigating an organization.

Covered entities and business associates should take steps to review their HIPAA compliance program, and refocus their breach prevention efforts and analyze their breach reporting processes. Organizations should ask the following questions: Are your safeguards sufficient to reduce the likelihood of improper PHI disposal or unwanted IT system intrusions? If your

organization has reported numerous breaches of the same type, have you made changes to existing procedures to reduce the likelihood of these breaches occurring again in the future? If your organization reports very few small breaches or none at all, do your workforce members fully understand what constitutes a breach, their reporting obligations, and does the organization properly analyze reported incidents?

An audit or review of your organization's HIPAA compliance program will help minimize the chance that your organization finds itself in the crosshairs of this new enforcement initiative. Contact INCompliance for further information about our HIPAA audit services by phone at 614.227.8938, by email at info@incomplianceconsulting.com or on our website at www.incomplianceconsulting.com.

The online HIPAA compliance program sponsored by Bricker & Eckler and INCompliance is available here, and comprehensive HIPAA information is available at the HIPAA Resource Center sponsored by Bricker & Eckler.

This Alert was prepared by Chris Bennington. If you have questions, please contact Chris at 513.870.6572 or cbennington@incomplianceconsulting.com. This and previous Alerts may be accessed on the INCompliance webpage.