"OCR expands PHI Investigations of Small Breaches"

"The Office for Civil Rights has announced it will "step up" the number of investigations into PHI breaches of fewer than 500 individuals."

The Department of Health and Human Services has announced that its Regional Offices for Civil Rights (OCR) will be increasing the number of investigations of breaches impacting fewer than 500 individuals (patient files) much more widely and with much closer scrutiny.

Until now, due to limited resources, investigations of small breaches (fewer than 500 individuals) have been performed as resources permitted, while OCR concentrated on PHI breaches that impact more than 500 individuals. While investigations of large-scale breaches of PHI will continue to be its priority, OCR's aim is to ensure that action is taken - by covered entities - to address non-compliance issues that lead to breaches of HIPAA Rules.

This announcement should serve as a warning to covered entities: OCR has previously opted to resolve non-compliance through voluntary actions by the covered entity. Even small data breaches can trigger HIPAA investigations and as you can see below, if OCR discovers HIPAA Rules have been violated, financial penalties can, and are likely to, be substantial.

In January 2013, OCR fined an Idaho hospice $50,000 following an investigation that involved the theft of an unencrypted laptop computer. The PHI breach affected 441 individuals.

A 2014 investigation of a QCA Health Plan breach of just 148 records resulted in a penalty of $250,000 plus the adoption of a corrective action plan. As with the Idaho investigation, this breach involved the theft of an unencrypted laptop computer.

In June of 2016, OCR fined a Philadelphia health care facility $650,000 following a PHI breach that impacted 412 individuals. Again, the investigation was triggered by the theft of a portable device containing patient PHI.

According to its release, Regional OCR Offices will consider a number of different factors while assessing breach reports and before initiating a breach investigation. These include the number of individuals (patients) that have been impacted by a breach; the types of data that have been exposed or stolen; whether data has been viewed or obtained by an unauthorized individual; whether a system used to store PHI has been infiltrated by a hacker; and the number of breach reports that have previously been submitted by the covered entity.