# GOVERNMENT INVESTIGATIONS INTO CYBERSECURITY BREACHES IN HEALTHCARE

Date: 11 February 2016

**Cyber Law and Cybersecurity Alert**

By: Eric M. Matava, Patricia C. Shea

In September 2015, a U.S. Department of Health and Human Services (HHS), Office of the Inspector General (OIG), report found that the Office of Civil Rights (OCR), the agency charged with ensuring compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), had not "fully implemented the required audit program to proactively assess possible noncompliance from covered entities." The HHS OIG report described OCR's oversight as "primarily reactive." As a result, the report recommended the implementation of a permanent audit program, scheduled to begin in early 2016. This development poses risks to healthcare providers faced with cybersecurity breaches and the potential for government investigations into the steps taken to address them.

In order to minimize exposure and prepare for any subsequent government investigation, healthcare providers must ensure that they have implemented the safeguards HIPAA requires. In the event these safeguards are unsuccessful in preventing a breach, healthcare providers must have an effective incident response plan in place. This article reviews the reporting obligations under HIPAA, provides an overview of state notification laws that may supplement HIPAA, reviews the potential consequences associated with noncompliance, and highlights several key steps for responding to a data breach.

Click here to read the full alert.

## KEY CONTACTS

**MARK A. RUSH**
PARTNER

PITTSBURGH, WASHINGTON DC
+1.412.355.8333
MARK.RUSH@KLGATES.COM



 