COSMOS
Navigate the Compliance Universe

# Compliance Today - June 2020
# Breach incident management: Providers should anticipate an OCR investigation

By Jan Elezian, MS, RHIA, CHC, CHPS, and Nancy Lipman, CCEP, CHC, CHPC

**Jan Elezian** (jan.elezian@sunhawkconsulting.com) is Director, SunHawk Consulting LLC in Denver, CO, and **Nancy Lipman** (nancy.lipman@cplc.org) is Vice President of Compliance at Chicanos Por La Causa Inc. in Phoenix, AZ.

- linkedin.com/in/jan-elezian-30821011/
- linkedin.com/in/nlipman/

With the implementation of the Breach Notification Rule under the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[1] the healthcare industry has experienced an increased risk of enforcement action by the Office for Civil Rights (OCR). Separate from the Breach Notification Rule, there are two additional factors compounding this risk. The first is individuals' ability to file a complaint directly with the OCR.[2] The OCR accepts all HIPAA violation complaints, from any source, about any covered entity or their business associate, regardless of the size or nature of the potential breach. The second is individuals' heightened awareness about the value of their personal information and the need to protect it. The OCR, in conjunction with law enforcement, investigates incidents involving theft of HIPAA protected information and fraud. Of the 91 reported breach incidents under investigation by the OCR during the first two months of 2020, 65 involved hacking or other information technology incidents, including those with potential malintent such as malware, ransomware, and phishing schemes.[3] Given any of these risk factors, it is practical to assume that there will be an OCR complaint filed for each compliance investigation conducted in response to an alleged breach. This article will discuss some key steps in managing a breach incident response.

## Recent examples

Three recent OCR settlements highlight the critical need for organizations to be knowledgeable and prepared to manage their response when a data breach is discovered.

- On May 6, 2019, the Tennessee-based Touchstone Medical Imaging entered into a $3 million settlement with the OCR when issues with risk analysis and management and timely breach notification to the Department of Health and Human Services, among other violations, were discovered during an OCR investigation.[4]
- On October 23, 2019, Jackson Health paid a $2.15 million civil monetary penalty when an OCR investigation revealed that multiple HIPAA violations were discovered within the health system, including a failure of risk management processes and failure to provide timely and accurate breach notification to the Department of Health and Human Services.[5]
- On November 27, 2019, Sentara Hospitals paid a $2.175 civil monetary penalty and agreed to a corrective action plan to settle HIPAA violations that included failure to accurately and timely report a data breach.[6]

While fines may be large due to many types of noncompliance variables that could present themselves during a data breach, in the above cases, large fines reflect the importance of reporting a known incident in a timely manner. Given that HIPAA investigations are often initiated by a complaint, organizations need to be mindful that the OCR will investigate not only the potential breach reported, but also how the organization responded once put on notice.