STRATEGIC MANAGEMENT SERVICES

HIPAA Breaches Now Occur on Average Once Per Day

By Richard Kusserow | April 9 2020 | HIPAA Compliance

Key Points:

- **Health care data breaches are increasing both in number and penalties.**
- **Most health care organizations have HIPAA Privacy under the Compliance Office.**

In the 2020 Compliance Benchmark Survey conducted by Strategic Management and SAI Global, 58% of respondents reported having HIPAA breach incidents involving the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) in the last 5 years. Also, three quarters of respondents reported that HIPAA Privacy was now the responsibility of the Compliance Officer. It is noteworthy that there has been a rapid increase in the number of breaches of patient privacy since 2016, many of which appear to be related to a continued growth in breaches due to third-party hacking, ransomware, and related malware incidents. In view of this, covered entities should focus on strengthening their IT systems to withstand attacks.

In 2019, OCR reported over $15 million in settlements for breaches. According to a report by the HIPAA Journal, health care data breaches involving nearly 39 million health care records had been reported to OCR by the end of 2019, which was more than double what was reported in all of 2018. In 2019, OCR published a Notification of Enforcement of Discretion explaining a change in its interpretation of the HITECH Act, leading to a change in policy. The revisions decreased limits for annual penalties in most culpability categories. OCR's penalties are based on four levels of culpability that consider the covered entity's knowledge of a violation and steps taken to mitigate the violation. Therefore, if a covered entity can show that it has mechanisms in place to prevent HIPAA breaches, such as regularly followed policies and procedures, the penalties imposed will be lower than what they would have been if no such policies and procedures were in place. On the other hand, if OCR finds that a covered entity acted with willful neglect when it came to its HIPAA duties, and failed to correct known inadequacies, then OCR will continue to penalize the covered entity with high dollar amounts. OCR has moved from a system where all types of culpability could lead to an annual penalty of maximum of $1.5 million to one where the annual limits for less culpable offenses is between $25,000 and $250,000.