Compliance Today - December 2019

Notable enforcement activity in 2019

by Jay P. Anstine

Jay P. Anstine (jay.anstine@bannerhealth.com) is the Area Compliance Program Director for Banner Health's Western Region Rural Hospitals.

As this year draws to a close, I wanted to take stock of the privacy world from an enforcement standpoint with the Department of Health and Human Services, Office for Civil Rights (OCR) to see what lessons can be learned. Below are some notable developments, as of the date of this writing (September 2019).

Notable enforcement activity

High-dollar settlements

For the OCR, 2019 began the same way 2018 ended, that is, a $3 million settlement. In December of 2018, OCR finalized a settlement with Cottage Health[1] related to two separate breaches involving an unprotected server. In May of 2019, OCR followed suit with a settlement with Touchstone Medical Imaging, Inc.[2] related to a file transfer protocol (FTP) server that allowed uncontrolled access to their patients' protected health information (PHI) over the internet.

Aside from the dollar amounts, some common themes included the organizations' lack of conducting an accurate and thorough risk analysis of potential risks and vulnerabilities to their ePHI, and failure to have business associate agreement(s)(BAA) in place. Touchstone went a step further in failing to timely respond to a known security incident.

Fines and penalties

In April, the OCR announced reducing the annual penalty caps across its four-tiered structure, except in instances of willful neglect.[3] This came on the heels of MD Anderson Cancer Center's appeal of an administrative law judge (ALJ) decision upholding civil remedies of approximately $4.3 million imposed against the organization. Central to the case were the organization's encryption policies that were in place beginning in 2006, but not adopted system-wide until 2011. In upholding the penalties, the ALJ took note of the organization's pace in complying with their own policies.

Right of access initiative

In September, the OCR announced a first-ever settlement with Bayfront Health St. Petersburg for $85,000 related to its Right of Access Initiative, a promise to enforce the rights of patients to timely receive copies of their medical records and not be overcharged.[4]

So what lessons can be learned as we move into 2020? First, take note of the common trends involving improper analysis of potential risks and vulnerabilities to ePHI, lacking BAAs, response times to known security incidents, and failing to follow policies. Additionally, as evidenced in the Bayfront Health St. Petersburg case, what the OCR says, the OCR does. Something to be mindful of as we move into 2020.