Report on Patient Privacy Volume 22, Number 4. April 07, 2022
Words From the Wise: OCR Shares Recurring Issues, Reviews Cases

By Theresa Defino

Over the past five years, the number of health care breaches affecting 500 or more individuals—deemed "large" breaches by the HHS Office for Civil Rights (OCR)—has doubled, and privacy and security violations reported by patients are also escalating.

More specifically, in 2021 OCR received 714 reports of large breaches, according to statistics presented by Yun-kyung Lee, deputy regional manager for OCR's pacific region, at the recent 26th annual Compliance Institute, sponsored by the Health Care Compliance Association, publisher of *RPP*.[1] In contrast, in 2017 there were 358, 2018 saw 369, 2019 had 512, and 2020 had 663, Lee said.

Causes of 500-and-over breaches have changed over time, as well. Lee's data encompassed the period from September 2009 through the end of last year and through the end of February. For the period from 2009 to 2021, the types of breaches, in order of occurrence, are hacking/information technology (43%), unauthorized access/disclosure (26%), theft (22%), loss (5%) and improper disposal and "other" (2% each).

From the start of this year until the end of February, the percentage of breaches stemming from hacking/information technology was 79%, with unauthorized disclosure a distant second at 19%. Looking at the location of breaches, the 2009-2021 data shows network servers (26%), email (21%), paper records (17%), laptops (9%), desktops and other (each 8%), portable electronic devices (4%) and electronic medical records (5%), Lee said.

Turning again to the first two months of this year and data for location, network servers have jumped up to 56%, followed by email (24%) and paper records (10%), according to data Lee presented.

For breaches affecting 500 or more individuals, OCR "look[s] into every one of those. We're looking at the underlying cause of the breach. We're looking at actions taken to respond to the breach incident" and "to prevent future incidents and the entity's compliance prior to the breach. So we're trying to figure out what happened, what could have been done beforehand that might have prevented this [and] what are you gonna do about it afterwards," said Lee.