Report on Patient Privacy Volume 19, Number 6. June 05, 2019 Generic 'Tester' Accounts Allowed Records Hack Triggering $1M in OCR, State AG Payments

By Theresa Defino

A large but short-lived 2015 breach of a medical records firm has resulted in two settlements totaling $1 million, demonstrating again that covered entities (CEs) and business associates (BAs) can expect both state and federal enforcement actions when data are exposed.

In a reversal of a more common situation, Medical Informatics Engineering (MIE) of Fort Wayne, Indiana, settled with the HHS Office for Civil Rights (OCR) for a far smaller amount ($100,000) than with a state agency. In this case, however, there were a total of 16 states involved—a first.

MIE settled with them for $900,000, according to a consent judgment and order entered May 23 into the U.S. District Court for the Northern District of Indiana, South Bend Division. On the same day, OCR announced its settlement. MIE is not completely out of the woods: a class action suit is still ongoing but may be settled soon, the company CEO told *RPP.*

Of the developments in this case, the state settlement is the most worthy of study and shows that the collective actions by state attorneys general pose new risk to CEs and BAs. The settlement also obligates MIE, a BA, to far more detailed and stringent requirements than are found in OCR's two-year corrective action plan (CAP) that could help serve as best practices for health care compliance officials. In addition, the suit contains more specifics about the breach and how MIE handled it.

The states' suit was filed in December 2018, led by Indiana Attorney General Curtis Hill and described by Hill's office as "the first time state attorneys general have joined together to pursue a HIPAA-related data breach case in federal court."

According to the settlement, MIE will pay the $900,000 in equal payments over three years. It did not admit to wrongdoing. In response to questions submitted by *RPP,* Douglas Horner, MIE's founder and CEO, calls the breach and resulting activities a "rollercoaster" that has resulted in valuable lessons worth sharing ("After Settlements, MIE CEO Shares Lessons Learned," *RPP* 19, no. 6).

In addition to Indiana, the states involved in the suit are Arizona, Arkansas, Connecticut, Florida, Kansas, Kentucky, Louisiana, Michigan, Minnesota, Nebraska, North Carolina, Tennessee, West Virginia, and Wisconsin. The attorney generals in these states allege that in addition to HIPAA, the breach violated state deceptive trade practices acts, state personal information protection acts, and state breach notification acts.