Report on Medicare Compliance Volume 28, Number 38. October 28, 2019
Vendor Oversight Is Up Because of Whaling; CEO Emails Are Reviewed

By Nina Youngstrom

A silent alarm goes off at Piedmont Healthcare in Atlanta when its vendors send an email or submit a form asking for their payments to be wired to a different account number. The request could be genuine, but the health system isn't taking any chances; it won't be granted without verifying the information. In the wake of reports that hackers have tricked executives at other organizations into authorizing money transfers to the criminals' bank accounts, which is variously known as whaling, CEO fraud and business email compromise, Piedmont Health has strengthened its vendor controls and monitoring.

"We won't just take a person who emailed the change as the source," says Debi Weatherford, executive director of internal audit at Piedmont Healthcare. "We go back to the known source at the vendor to make sure the form came from them and they requested the change."

The frequency of wire transfers and automated clearing house (ACH) payments reinforces the need for vendor controls and oversight, she says. "Until you start looking, you don't identify opportunities to improve your controls."

Using a questionnaire,[1] the internal audit department at Piedmont audits the controls regularly to ensure processes are followed. "Our role is to make sure internal controls are effective and address the risks for the organization," Weatherford notes. For example, if a pharmaceutical company emails a change form for a wire transfer or ACH payment and the account number is off by one number, an independent person should call the drug company's known contact and confirm that the requested change and the account number are valid. "You want to segregate your duties in the vendor controls process," she advises. "Validation needs to occur in another department that did not receive the requested change for the update to the vendor file and change in payment address."