Report on Medicare Compliance Volume 31, Number 5. February 07, 2022

As a Gateway to ePHI and Provider Banking Information, Payer Websites Are Ripe for Audit

By Nina Youngstrom

Knowing that people at health care organizations are able to execute electronic fund transfers on payer websites and access electronic protected health information (ePHI), Ochsner Health in New Orleans grew concerned. It decided the time had come for an audit of access controls on the payer portals, which contain patient and financial information.

Websites for payers like UnitedHealthcare, Anthem and Cigna are used for revenue cycle processes—preauthorization requests, claims submissions and payments, said Kelly Rollins, manager of IT audit at Ochsner. They could be a conduit for a breach because they provide access to ePHI or theft because payers use the portals to make payments to providers through electronic funds transfer/electronic remittance advice (EFT/ERA). It may take a diversion or something close to it for health care organizations to recognize that insurance websites represent another source of HIPAA and financial risk, she said. That's why a different kind of audit and response is necessary.

"Addressing potential financial and patient risks were the drivers for this audit," Rollins said.

To get Ochsner's audit of payer websites underway, Rollins asked the revenue cycle department to identify the population (payers with websites) and Ochsner's tax identification numbers (TINs) and national provider identifiers (NPIs). Because there are hundreds of payers, it may be necessary to take a risk-based approach to auditing. "Some of these payer websites are considered self-applying," Rollins said. In other words, anyone with a TIN was able to create an account and access the payer website. "That's where we started. We focused on websites that didn't require authorization or approval from the user perspective from Ochsner. That was the scope," she said.