Report on Patient Privacy Volume 18, Number 11. November 30, 2018
Privacy Briefs: November 2018

By HCCA Staff

◆ The Employee Retirement System of Texas reported to the HHS Office for Civil Rights on Oct. 15 that information on possibly 1.25 million people may have been exposed in a health data breach involving the ERS password-protected portal, ERS OnLine. "A now-corrected security flaw allowed certain ERS members who logged in with their username and password, and used a specific function to input search criteria, to view some member information that was not theirs," ERS said in a statement. Members might have been able to see first and last names, Social Security numbers, and ERS member identification numbers for a limited group of members. However, ERS said fraudulent use of the information was unlikely. "We are making people aware of the issue because there's a slight possibility some ERS members might have seen their fellow members' information, and because we take your privacy and data security very seriously," ERS said.

◆ State Medicaid agencies and contractors identified 1,260 data breaches in 2016, but those breaches typically affected few beneficiaries, according to a report from the HHS Office of Inspector General (OIG). The report found breaches "often resulted from misdirected communications, such as letters and faxes, and exposed beneficiaries' names and Medicaid or other identification numbers." Breaches that resulted from hacking or other information technology-related incidents were rare, the report said. The OIG recommended that the Centers for Medicare & Medicaid Services reissue guidance to states about reporting Medicaid breaches to CMS, and said that collecting information on a national scale regarding Medicaid data breaches could help CMS identify breach trends and promote effective state responses. Read the full report at https://bit.ly/2OAOhde.

This document is only available to subscribers. Please log in or purchase access.

Purchase Login