# Report on Patient Privacy Volume 23, Number 2. February 09, 2023 Privacy Briefs: February 2023

By Jane Anderson

◆ **DCH Health Systems, based in Tuscaloosa, Ala., said it fired an employee in December after a routine privacy audit revealed evidence that the worker had accessed some 2,530 patient electronic medical records without a legitimate reason.** The information that may have been accessed and viewed without authorization contained the following data elements: name, address, date of birth, Social Security numbers, dates of provider encounters, diagnoses, vital signs, medications, test results, and clinical/provider notes, DCH Health Systems said in a breach notification posted on its website. The initial routine audit found evidence that the employee had accessed one patient's records on Dec. 5, the health system said. "Upon identifying the initial inappropriate access, DCH Health System immediately suspended the employee and terminated the employee's access to all medical records and other information systems. Upon further investigation to assess the information impacted, DCH subsequently terminated the individual's employment one business day after initial discovery." It also engaged a data breach recovery expert and "established all required and necessary communications to the affected patients and regulatory officials," the health system said. It also will offer free identity theft protection services to all patients whose insurance group and subscriber/policy numbers may have been involved.[1]