"Labs Should Heed Lessons from Huge Data Breach"

James J. Giszczak | Monday, July 1, 2019

PHI of 20 million patients from four of nation's largest clinical lab companies was compromised

CEO SUMMARY: Following news last month about the biggest breach of personal health information in the clinical lab industry, lawyers representing some of the affected patients filed at least 12 class action lawsuits. Federal officials and attorneys general in multiple states also launched investigations. The breach occurred when hackers gained access to the data systems of a bill-collector vendor used by the four lab companies. An attorney advised clinical labs to review how they and their vendors handle PHI.

DATA BREACHES AFFECTING TWENTY MILLION PATIENTS of four of the nation's largest laboratory companies are classic examples of why healthcare providers need to monitor the work vendors do on their behalf.

In June, these clinical laboratory companies reported breaches of personal health information (PHI):

BioReference Laboratories (a subsidiary of Opko Health),
Laboratory Corporation of America,
Quest Diagnostics, and

Sunrise Laboratories (a division of Sonic Healthcare USA).

The laboratory companies had sent patients' data to the American Medical Collection Agency (AMCA), a medical bill and debt collector in Elmsford, N.Y. These labs were among AMCA's largest clients, according to published reports. Within days of the announcement of the breach, AMCA filed for protection under Chapter 11 of the U.S. Bankruptcy laws.(See "BRLI, LabCorp, Quest Disclose Data Breaches of 20M Patients," TDR, June 10, 2019.)

In its filing with the U.S. Bankruptcy Court for the Southern District of New York, AMCA said its data were hacked over seven months from about Aug. 1, 2018, to March 30 of this year. The hackers stole patients' records from the four lab clients, plus CareCentrix (a home care provider).

In June, attorneys general in at least six states—Connecticut, Illinois, Michigan, Minnesota, North Carolina, and New York—said they were investigating the breach.

Stolen Data Offered For Sale

Hackers collected patients' names, Social Security numbers, addresses, dates of birth, and payment card information, all of which was later advertised for sale in underground web forums, according to reporting by Charlie Osborne of ZD Net.

To help lab managers and pathologists understand their lab's responsibilities to safeguard patients' PHI under federal and state laws, The Dark Report interviewed James Giszczak, an attorney and co-chair of the Data Privacy and Cybersecurity Group, at McDonald Hopkins.

"One important lesson from this data breach is how critical it is for clinical labs and pathology groups to be proactive in making sure they review their vendor agreements," said Giszczak. "In that review, labs need to know the specific measures each vendor is taking to protect the information the lab is providing to their vendors."

Click here to read the full article from The Dark Report.

James J. Giszczak