Hawthorn Physician Services 10820 Sunset Office Drive, 3rd Floor, St. Louis, MO, 63127 314-238-5216

Security Breaches Could Reach All-Time High This Year

Ongoing data hacks at AMCA have impacted Quest and LabCorp

Through the first half of 2019 the healthcare industry has reported numerous data breaches, with over 25 million patient records compromised.

A partial list of healthcare data breaches through June of 2019 includes: Inmediata Health Group, University of Washington Medicine, Columbia Surgical Specialists of Spokane, UConn Health and the Oregon Department of Human Services.

The largest breach occurred at American Medical Collections Agency (AMCA), a firm specializing in patient balances. AMCA was hacked between August 2018 and March 2019, with over 20 million patients impacted. Patient records for both Quest and LabCorp were compromised. (Quest at 12 million patients affected, and LabCorp at 7.7 million patients affected.)

According to Chief Privacy Officer magazine, as of the end of June, only 200,000 patients have been notified directly and told about the AMCA breach. The Health Insurance Portability and Accountability Act (HIPAA) requires that patients must be notified within 60 days after a data breach discovery.

While Quest and LabCorp account for the largest number of patients affected by the AMCA breach, a number of additional companies and medical practices have issued press releases informing the public about their compromised patient records. These firms include Sunrise Medical Laboratories, Arizona Dermatopathology, Seacoast Pathology, South Texas Dermatopathology, and Austin Pathology Associates.

As reported previously in Hawthorn publications, the healthcare sector is a frequent target for cyber criminals. In addition to healthcare provider information, hackers can obtain patients' Social Security numbers and email addresses, along with information about bank accounts, credit cards and debit cards. Once this information is sold through encrypted sites on the dark web, criminals can deploy methods to monetize the information.

Shelly Bangert, Hawthorn's director of revenue cycle management, commented on ways criminals defraud patients. "Data breaches give criminals the information they need to send emails with fake invoices to patients" Bangert said. "They can cite the precise dates of medical treatment and ask patients to submit payments. It's a tragic situation that underscores the importance of maintaining high levels of data security."

Maximum Security is a promise of the Hawthorn Advantage. Our safeguards protect patients' and physicians' confidential data.

We have achieved a record of 100% success in preserving confidentiality.

Hawthorn Physician Services can maximize your security while increasing your revenue and profit. Please visit www.hawthorngrp.com to learn more.

HAWTHORN
PHYSICIAN SERVICES CORPORATION

Addressing Complexity with Certainty