**Mobile App of Quest Diagnostic Compromised 34,000 records in a Security Breach**

Recently, Quest Diagnostics suffered data breach which led to the leakage of health records of 34,000 people. The breach occurred due to a vulnerability in the company’s mobile app. The app, called MyQuest, is not only web based but also available for Android and Apple devices.

According to a statement issued by the company, "On November 26, 2016 an unauthorized third party accessed the MyQuest by Care360 internet application and obtained Protected Health Information (PHI) of approximately 34,000 individuals. The accessed data included name, date of birth, lab results, and in some instances, telephone numbers. The information did not include Social Security numbers, credit card information, insurance or other financial information. There is no indication that individual’s information has been misused in any way."

Quest Diagnostics said that the customers affected by the breach have been notified and the company is investigating the breach along with taking preventive measures of mobile app security testing to prevent further breach incidents. It said, "Quest is taking steps to prevent similar incidents from happening in the future, and is working with a leading cybersecurity firm to assist in investigating and further evaluating the company's systems. The investigation is ongoing and the unauthorized intrusion has been reported to law enforcement."

The MyQuest app, formerly known as Gazelle, is being offered since 2010. When first introduced, it made headlines for putting up lab test results in a mobile app before they even appeared online. A one of its kind useful app for patients, it lets them schedule appointments, get lab results, integrate data from wearable sensors and keep a record of their medication timings.

With data breaches like this on the rise in healthcare, mobile app security testing is a need of the hour for companies that hold critical patient data. A mobile app being the reason of a data breach as large as this one calls for companies to raise their security and privacy concerns and introduce secure mobile apps only after ongoing mobile app security testing.