COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 19, Number 11. November 07, 2019 Patient Privacy Court Case: November 2019

By Wogai Mohmand

Quest Diagnostics Data Breach Settlement Approved

On October 25, a federal judge in New Jersey gave her initial approval to a $195,000 settlement deal in a proposed class action against Quest Diagnostics Inc. The plaintiffs' claims arose out of a data breach in which protected health information (PHI) of about 34,000 Quest Diagnostics Inc. patients was exposed to a third party in November 2016.

The breach occurred when an unauthorized third party accessed the MyQuest by Care360 internet application on Nov. 26, 2016. MyQuest is a service offered by Quest Diagnostics to its patients that allows them to receive and view their lab results. The unauthorized third party obtained PHI from this application that included names, dates of birth, lab results, and, in some instances, telephone numbers. The affected information did not include Social Security numbers, credit card information, insurance, or other financial information.

On Dec. 12, 2016, Quest publicly announced the data breach and notified affected customers individually by letter of the breach. The class action against Quest was filed nine days later. The suit alleged that Quest failed to safeguard its clients' information, and that Quest's approach to maintaining the privacy of its patients and protecting health information "was lackadaisical, cavalier, reckless or at the very least negligent." The plaintiff claimed that the class members "have been placed at an imminent, immediate and continuing increased risk of harm from identity theft and identity fraud."

Ten days after a motion was filed to approve a class settlement, U.S. District Judge Claire C. Cecchi granted the settlement, stating that it was "fundamentally fair, reasonable, adequate and is in the best interests" of the settlement class members. The briefing for the settlement proposal acknowledged that the uncertain nature of data breach cases makes such cases risky and their litigation unpredictable because class certification is rare. The plaintiffs claimed that the lack of direct precedent in data breach suits created an additional risk in achieving and maintaining a class action, and was thus partially why the class members sought approval of the settlement. Under the settlement, all individuals, with a few exceptions, residing in the United States whose personal information was obtained by an unauthorized third party in the incident are eligible for a payment. Each eligible class member could receive a maximum reimbursement of $325.

[1]