DORSEY
DORSEY+WHITNEY LLP

DOJ Announces First Settlement Under New Civil Cyber-Fraud Initiative

March 28, 2022 – FCA Now
by Erica Andrews

In October 2021, the Department of Justice ("DOJ") announced its new Civil Cyber-Fraud Initiative, led by the Civil Division's Fraud Section, to enhance its ongoing efforts to address cybersecurity threats. The initiative utilizes the False Claims Act ("FCA") to prosecute cybersecurity fraud by federal contractors and grant recipients who put government information or systems at risk through deficient cybersecurity standards. Cybersecurity risks that the initiative will pursue include knowingly providing deficient cybersecurity products or services, knowingly misrepresenting cybersecurity practices or protocols, and failure to monitor and report cybersecurity incidents and breaches.

This month, DOJ settled its first case under the new initiative. Florida-based Comprehensive Health Services ("CHS") agreed to pay $930,000, in part to resolve FCA allegations related to cyber fraud. The settlement also resolved FCA claims that alleged CHS provided medical supplies that were not approved by the U.S. Food and Drug Administration ("FDA") or the European Medicines Agency ("EMA") as required by their federal contracts.

CHS is a medical services provider that has contracts to provide medical support services at State Department and Air Force facilities in Iraq and Afghanistan. Pursuant to these contracts, CHS submitted claims to the State Department for the cost of a secure electronic medical record ("EMR") system, which was used to store patient medical records in an agency run medical facility in Iraq.

This EMR system housed patient records containing confidential identifying information of U.S. service members, U.S. diplomats, government officials, and contractors. The DOJ alleged that CHS did not exclusively retain these confidential medical records on the EMR system, however, as they were required to under their contract. Instead, the DOJ alleged that the company left copies of the patient records on an internal network drive, which could be accessed by non-facility staff, between 2012 and 2019. This practice allegedly continued even after facility staff raised concerns about the breach in 2017, with CHS failing to disclose to the government this non-exclusive storage of patient

Related Capabilities

- Healthcare Enforcement & Compliance
- Government Enforcement & Corporate Investigations

records on a secure EMR system. The government was alerted to the alleged practices by a relator prior to filing its complaint in 2019.

A key takeaway here is that government contractors and grant recipients must ensure that their cybersecurity practices are up to the standards required under their federal contracts. They should ensure not only that their products and systems are up to date and proper policies are in place to address cyber security risks, but also that those policies are followed in practice, and any breach must be promptly disclosed to the government. The Civil Cyber-Fraud Initiative is yet another avenue for FCA enforcement, and for the government to ensure those receiving its funds are appropriately securing its data.