Published on *The National Law Review* https://natlawreview.com

Well, That Didn't Take Long – DOJ Announces its First Settlement of a Civil Cyber-Fraud Case

Article By:

Townsend L. Bourne

Nikole Snyder

On March 8, 2022, just five months after the creation of the Department of Justice's ("DOJ") new Civil Cyber-Fraud Initiative (previously discussed here), the DOJ announced its first settlement of a cyber-related fraud case. Under the settlement agreement, Comprehensive Health Services LLC ("CHS") will pay $930,000 to resolve whistleblower allegations that it violated the False Claims Act by (among other things) failing to properly store and handle confidential information. This likely is just the start for increased cyber-related enforcement actions.

CHS had contracts to provide medical support services at government facilities in Iraq and Afghanistan. As described in the settlement agreement, CHS failed to properly store patient medical records on a secure electronic medical record ("EMR") system as required by its contract, while at the same time submitting claims for payment to the government for the cost of a secure EMR system. In particular, CHS staff allegedly saved and left copies of some medical records on an internal network drive that was accessible to non-clinical staff. Additionally, as set forth in the settlement agreement, after concerns were raised internally CHS failed to take adequate steps to properly and securely store the information on the EMR system and failed to disclose to the Government that it had not securely stored such records. The settlement also describes allegations that CHS provided patients with controlled substances that were unapproved by the U.S. Food and Drug Administration ("FDA") or European Medicines Agency ("EMA"), and falsely represented such substances were approved.

Although this particular case involves medical records, it is not likely to be long before we see enforcement actions against federal contractors that handle or store other types of confidential or sensitive government information on their systems. Federal contractors have cybersecurity obligations under existing regulations to protect federal contract information and controlled unclassified information ("CUI"), and many Department of Defense contractors have additional obligations to protect and perform cybersecurity assessments relating to covered defense information (a type of CUI). It is not hard to imagine the potential for a significant False Claims Act case against a defense contractor that performs a subpar assessment and/or misreports the results of an assessment, particularly where submission of every invoice to the government may constitute an implied certification that the company is compliant with all contractual cybersecurity obligations.

In its press release, the DOJ highlighted this settlement as a demonstration of “the department’s commitment to use its civil enforcement tools to pursue government contractors that fail to follow required cybersecurity standards,” and noted that it “will continue to ensure that those who do business with the government comply with their contractual obligations, including those requiring the protection of sensitive government information.” Contractors should take immediate note and ensure any representations made regarding the security of information systems housing sensitive government information are current and accurate.

National Law Review, Volume XII, Number 69