CARLTON FIELDS

DOJ's First Cyber-Fraud Settlement Places Emphasis on Cybersecurity Shortfalls

March 21, 2022

Last year, the Department of Justice (DOJ) unveiled its Civil Cyber-Fraud Initiative, intended to ensure compliance, by leveraging the False Claims Act (FCA), with contractual cybersecurity requirements applicable to government contractors.

On March 8, the DOJ settled allegations in two FCA qui tam complaints against Comprehensive Health Services LLC (CHS), a provider of global medical services, marking the first resolution of such a case after the launch of the Civil Cyber-Fraud Initiative.

Between 2011 and 2021, CHS submitted proposals for, and was awarded, federal contracts, which required them to provide medical support services to government-run facilities overseas. Under one of the contracts, CHS was required to provide a secure electronic medical record (EMR) system to store all patients' medical records, including confidential identifying information of U.S. service members, diplomats, officials, and contractors working and receiving medical care overseas. However, CHS did not consistently store records on a secure EMR system. Instead, CHS left copies of medical records and identifiable information on an internal network drive, which non-clinical staff could have accessed. Although staff raised concerns about the privacy of such sensitive information, CHS did not take adequate steps to store that information exclusively on the EMR. Throughout this period, CHS billed the Department of State $485,866 for the EMR.

In addition, CHS' contracts with the federal government also required the company to provide medical supplies, including controlled substances approved by the U.S. Food and Drug Administration (FDA) or the European Medicines Agency (EMA). But, during the relevant time frame, CHS stated certain substances were approved by the FDA and the EMA while lacking a drug enforcement agency license necessary for exporting such substances from the United States to Iraq.

Under the settlement agreement, CHS did not admit liability but agreed to pay $930,000 to resolve violations of the FCA for inaccurately reporting that it met contract requirements for supplying medical services to government-run facilities overseas.

Albeit the first of its kind, this settlement demonstrates the DOJ's "commitment to use its civil enforcement tools to pursue government contractors that fail to follow required cybersecurity standards, particularly when they put confidential medical records at risk." The DOJ is prepared to "ensure that those who do business with the government comply with their contractual obligations, including those requiring the protection of sensitive government information," and we expect to see many more of these cyber-related FCA enforcement actions in the near future.

Key Takeaways

Government contractors may reduce their risk of an FCA claim related to allegedly lax cybersecurity by implementing traditional compliance reviews focused on cybersecurity requirements. For example:

1. Review and understand the cybersecurity requirements that apply to your contracts. Awareness of the specific cybersecurity requirements that apply to your contract is the first step toward compliance. Engaging counsel to understand requirements that are unclear before certifying compliance may negate claims that the contractor acted with reckless disregard as to its cybersecurity obligations or knowingly violated those obligations.
2. Assess your system(s) to ensure compliance with your cybersecurity obligations. A critical examination of your system(s) can identify weaknesses related to any contractual cybersecurity requirements.
3. Use assessment findings to establish appropriate internal controls, audits, and reporting mechanisms. Ensuring that you remain in compliance with any cybersecurity provisions is critical for the life of the contract. Regular audits and internal controls can identify and correct issues before cybersecurity recertification. Moreover, the FCA punishes retaliation against whistleblowers and encourages people to report cyber-related fraud to the DOJ. To encourage employees to promptly report any concerns directly to the company, contractors should ensure a method exists for reporting cybersecurity issues internally and should promptly remedy any reported concerns.

4. Maintain an incident response plan that includes promptly evaluating reporting obligations to the government. An incident response plan is a company's playbook that outlines how cyber incidents are detected, reported, investigated, and remediated. This plan identifies team members, roles, and responsibilities. In this way, a plan can help a company identify and respond to cyber incidents quickly and effectively, which is paramount for not only addressing the threat but also fulfilling any government reporting obligations.

Authored By

Adam P. Schwartz

Erin J. Hoyle

Eden Marcu

Related Practices

White Collar Crime & Government Investigations
Cybersecurity and Privacy
Health Care

Related Industries

Health Care

accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.