



PRESS RELEASE

Contractor Pays \$930,000 to Settle False Claims Act Allegations Relating to Medical Services Contracts at State Department and Air Force Facilities in Iraq and Afghanistan

Tuesday, March 8, 2022

For Immediate Release

U.S. Attorney's Office, Eastern District of
New York

First Settlement of a Civil Cyber-Fraud Case Under the Department of Justice's Civil Cyber-Fraud Initiative

BROOKLYN, NY – Comprehensive Health Services, LLC (CHS), located in Florida, has agreed to pay \$930,000 to resolve allegations that it violated the False Claims Act by falsely representing to the State Department and the Air Force that it complied with contract requirements relating to the provision of medical services at State Department and Air Force facilities in Iraq and Afghanistan. This is the Department of Justice's first resolution of a False Claims Act case involving cyber fraud since the launch of the Department's Civil Cyber-Fraud Initiative, which aims to combine the Department's expertise in civil fraud enforcement, government procurement, and cybersecurity to combat new and emerging cyber threats to the security of sensitive information and critical systems

Breon Peace, United States Attorney for the Eastern District of New York; Brian M. Boynton, Principal Deputy Attorney General of the Justice Department's Civil Division; Roger B. Handberg, United States Attorney for the Middle District of Florida; Elisabeth "Elli" Kaminsky, Special Agent-in-Charge, United States Department of State, Office of Investigations; and Nicholas J. Groesbeck, Special Agent-in-Charge, Air Force Office of Special Investigations, Procurement Fraud Detachment 4, Wright-Patterson AFB, Ohio (OSI), announced the settlement.

CHS is a provider of global medical services that contracted to provide medical support services at government-run facilities in Iraq and Afghanistan. Under one of the contracts, CHS submitted claims to the State Department for the cost of a secure electronic medical record (EMR) system to store all patients' medical records, including the confidential identifying information of United States service members, diplomats, officials, and contractors working and receiving medical care in Iraq. The United States alleged that, between 2012 and 2019, CHS failed to disclose to the State Department that it had not consistently stored patients' medical records on a secure EMR system. When CHS staff scanned medical records for the EMR system, CHS staff saved and left scanned copies of some records on an internal network drive, which was accessible to non-clinical staff. Even after staff raised concerns about the privacy of protected medical information, CHS did not take adequate steps to store the information exclusively on the EMR system.

The State Department and Air Force contracts also required CHS to provide medical supplies, including controlled substances, that were approved by the U.S. Food and Drug Administration (FDA) or European Medicines Agency (EMA) and manufactured in accordance with federal quality standards. The United States alleged that, between 2012 and 2019, CHS falsely represented to the State Department and Air Force that certain substances provided under those contracts were approved by the FDA or EMA. CHS lacked a Drug Enforcement Agency license necessary for exporting controlled substances from the United States to Iraq. CHS obtained controlled substances by having CHS physicians based in Florida send letters requesting that a South African physician prescribe the controlled substances. A South African shipping company then received controlled substances that were not approved by the FDA or EMA and sent them to CHS in Iraq, where CHS supplied the unapproved controlled substances to patients under the State Department and Air Force contracts.

"Protecting the health and safety of servicemembers, diplomats, and other government employees working abroad is of utmost importance. The defendants were required to maintain personal health information securely and provide only approved pharmaceuticals to patients. This settlement serves notice to federal contractors that they will be held accountable for conduct that puts private medical records and patient safety at risk," stated United States Attorney Breon Peace for the Eastern District of New York. "We are grateful for the support of our colleagues in the Middle District of Florida, the State Department, and the Air Force for their assistance in investigating these important claims."

“This settlement demonstrates the department’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,” stated Principal Deputy Assistant Attorney General Brian M. Boynton of the Justice Department’s Civil Division. “We 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.”

“Government contractors should never disregard their obligations when providing medical care to members of the military,” stated United States Attorney Roger B. Handberg for the Middle District of Florida. “We thank our colleagues in the Eastern District of New York, as well as the investigative agencies who supported this effort, for their steadfast pursuit of this important investigation.”

“This settlement demonstrates the commitment State Department, Office of Inspector General, Special Agents have to protect the safety, well-being, and personal information of State Department personnel. Our hope is that this outcome will send a clear message that cutting corners on State Department contracts has significant consequences.” stated Special Agent in Charge Elisabeth “Elli” Kaminsky of the U.S. Department of State OIG, Office of Investigations.

“The Department of the Air Force Office of Special Investigations (OSI) is undeterred in its approach to hunting down fraud within our Foreign Military Sales programs and ensuring the offenders are held accountable,” stated Air Force OSI Special Agent-in-Charge Groesbeck. “We applaud the complainant for coming forward, which allowed our joint partners to protect the governments procurement process and carry out the warfighting mission.”

The civil settlement includes the resolution of two actions brought under the *qui tam* or whistleblower provisions of the False Claims Act against CHS. Under the *qui tam* provisions of the False Claims Act, a private party can file an action on behalf of the United States and receive a portion of the settlement if the government takes over the case and reaches a monetary agreement with the defendant. The *qui tam* cases are captioned *United States ex rel. Lawler v. Comprehensive Health Servs., Inc. et al.*, Case No. 20-cv-698 (E.D.N.Y.) and *United States ex rel. Watkins et al. v. CHS Middle East, LLC*, Case No. 17-cv-4319 (E.D.N.Y.).

The investigation and resolution of this matter demonstrates the government’s emphasis on combatting cyber-fraud. On October 6, 2021, the Deputy Attorney General announced the [Department’s Civil Cyber-Fraud Initiative](#), which aims to hold accountable entities or individuals that put U.S information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches. Information on how to report cyber fraud can be found [here](#).

The resolutions obtained in this matter were the result of a coordinated effort between the United States Attorney's Office for the Eastern District of New York, the Fraud Section of the Commercial Litigation Branch of the Justice Department's Civil Division, the U.S. Attorney's Office for the Middle District of Florida, the United States Department of State Office of Inspector General, and the United States Air Force.

The claims resolved by the settlement are allegations only and there has been no determination of liability.

The government's case was handled by Assistant U.S. Attorney Christopher Volpe and former Assistant U.S. Attorney Lisa Kutlin of the Eastern District of New York, and Assistant U.S. Attorney Jeremy Bloor of the Middle District of Florida.

Contact

John Marzulli
Danielle Blustein Hass
United States Attorney's Office
(718) 254-6323

Updated March 8, 2022

Topics

CYBERCRIME

FALSE CLAIMS ACT

Component

[USAO - New York, Eastern](#)

Related Content

PRESS RELEASE

Long Island Man Sentenced to 28 Years in Prison for Sexually Exploiting Minors

Earlier today, at the federal courthouse in Central Islip, Edgardo Mejia was sentenced by United States District Judge Joan M. Azrack to 28 years in prison for sexually exploiting minors. The...

October 24, 2024

PRESS RELEASE

Dark Web Vendor Pleads Guilty to Distributing Fentanyl Through the Mail

Earlier today, in federal court in Brooklyn, Ryan Scott Cochran, also known as “namedeclined,” pleaded guilty to distributing fentanyl, cocaine and methamphetamine through the United States mail. Today’s proceeding was...

August 28, 2024

PRESS RELEASE

Four Individuals Charged in Connection With Business Email Compromise Schemes and Related Romance Schemes

Today, indictments were unsealed in federal court in Brooklyn charging four defendants for their participation in a series of fraudulent business email compromise schemes and related romance schemes that resulted...

June 12, 2024



Eastern District of New York

Main Office

271 Cadman Plaza East

Brooklyn NY 11201



Telephone: 718-254-7000

Fax Line: 718-254-7508