COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 4. April 06, 2023 Florida Web Designer Settles with DOJ on 2020 HealthyKids.org Medicaid Breach

By Jane Anderson

A Florida communications firm and its owner agreed to pay $293,771 to resolve False Claims Act (FCA) allegations that they failed to secure personal information on a federally funded Florida children's health insurance website, HealthyKids.org.

The March 14 settlement[1] against Jelly Bean Communications Design LLC represents the third action in the U.S. Department of Justice's (DOJ'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.

Two of the three initiative actions have involved health care entities, and so this effort provides another way—separate from actions by the HHS Office for Civil Rights—for the federal government to hold health care entities accountable for major security lapses that reveal individuals' personal information.

"Government contractors responsible for handling personal information must ensure that such information is appropriately protected," said Principal Assistant Attorney General Brian Boynton, head of DOJ's Civil Division.

In October 2013, the Florida Healthy Kids Corporation (FHKC), a state-created entity that offers health and dental insurance for Florida children ages five through 18, contracted with Jelly Bean for "website design, programming and hosting services." FHKC receives Medicaid and state funds to provide children's health insurance programs.

The agreement with FHKC required that Jelly Bean provide a fully functional hosting environment that complied with the protections for personal information imposed by HIPAA; Jelly Bean agreed to adapt, modify and create the necessary code on the webserver to support the secure communication of data, DOJ said. Jeremy Spinks, the company's manager, 50% owner and sole employee, signed the agreement.

Jeally Bean "Did Not Provide Secure Hosting"

Under its contracts with FHKC, between 2013 and 2020, Jelly Bean created, hosted and maintained HealthyKids.org for FHKC, including the online application into which parents and others entered data to apply for state Medicaid insurance coverage for children.

The settlement resolves allegations that from Jan. 1, 2014, through Dec. 14, 2020, "contrary to its representations in agreements and invoices, Jelly Bean did not provide secure hosting of applicants' personal information and instead knowingly failed to properly maintain, patch, and update the software systems underlying HealthyKids.org and its related websites, leaving the site and the data Jelly Bean collected from applicants vulnerable to attack," DOJ said.

"In or around early December 2020, more than 500,000 applications submitted on HealthyKids.org were revealed to have been hacked, potentially exposing the applicants' personal identifying information and other

data," DOJ said.

At the time, FHKC said that the incident involved access and tampering with the applications for "several thousand" Medicaid applicants.[2]

After its investigation, FHKC said, "cybersecurity experts identified significant vulnerabilities in the hosted website platform and the databases that support the online FloridaKidCare application. FHKC learned that these vulnerabilities spanned a seven-year period from November 2013 until December 2020."

The information that may have been exposed included full names, dates of birth, email addresses, phone numbers, addresses, Social Security numbers, financial information and secondary insurance information. However, Jelly Bean did not maintain adequate audit logs showing who accessed applicants' personal information, DOJ said.

Software Was Not Updated or Patched

DOJ alleged that Jelly Bean was running multiple outdated and vulnerable applications, including some software that Jelly Bean had not updated or patched since November 2014. "Inconsistent with its representations in the agreements and invoices, Jelly Bean did not provide secure hosting of applicants' personal information and instead failed to properly maintain, patch, and update the software systems underlying HealthyKids.org and its related websites, leaving the site and the data Jelly Bean collected from applicants vulnerable to attack," DOJ said in its settlement agreement.[3]

In response to the data breach and Jelly Bean's cybersecurity failures, FHKC shut down the website's application portal in December 2020, DOJ said.

One of the two prior Civil Cyber-Fraud Initiative settlements involved a Florida health care entity. In that one, Comprehensive Health Services LLC (CHS), based in Cape Canaveral, Florida, agreed in March 2022 to pay $930,000 to resolve allegations that it violated the FCA by falsely representing to the U.S. State Department and the Air Force that it complied with contract requirements relating to the provision of medical services at facilities in Iraq and Afghanistan.[4]

According to that settlement, CHS, a provider of global medical services, 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 U.S. service members, diplomats, officials and contractors working and receiving medical care in Iraq.

DOJ alleged that, between 2012 and 2019, CHS failed to disclose to the State Department that it had not consistently stored patients' records on a secure EMR system. When CHS staff scanned medical records for the EMR system, staff also saved and left scanned copies of some records on an internal network drive, which was accessible to nonclinical 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," DOJ said.

The second Civil Cyber-Fraud Initiative settlement, announced in July 2022, involved Aerojet Rocketdyne Inc., a California contractor working with the U.S. Department of Defense, NASA and other federal agencies.

1 U.S. Department of Justice, "Jelly Bean Communications Design and its Manager Settle False Claims Act Liability for Cybersecurity Failures on Florida Medicaid Enrollment Website," news release, March 14, 2023, https://bit.ly/3Lvosb1.

2 Jane Anderson, "Privacy Briefs: February 2021," *Report on Patient Privacy* 21, no. 2 (February 2021), https://bit.ly/42nPffh.
3 U.S. Department of Justice v. Jelly Bean Communications Design LLC and Jeremy Spinks, "Settlement Agreement," March 14, 2023, https://bit.ly/3Tp0aRQ.
4 U.S. Department of Justice, "Medical Services 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," news release, March 8, 2022, https://bit.ly/3ZWWnxL.