Security flaws found in three state health insurance websites

April 7 2016, by Adam Beam And Ricardo Alonso-Zaldivar

In this Oct. 1, 2013 file photo, workers at the Vermont Health Connect call center talk to customers in Burlington, Vt. The U.S. Government Accountability Office confirmed Thursday, April 7, 2016, that the state health insurance exchanges in Vermont, Kentucky and California had cybersecurity weaknesses in their health insurance exchanges, potentially exposing to hackers electronic systems that contain sensitive personal information on hundreds of thousands of consumers. (AP Photo/Toby Talbot, File)

Federal investigators found significant cybersecurity weaknesses in the

health insurance websites of California, Kentucky and Vermont that could enable hackers to get their hands on sensitive personal information about hundreds of thousands of people, The Associated Press has learned. And some of those flaws have yet to be fixed.

The vulnerabilities were discovered by the Government Accountability Office, the investigative arm of Congress, and shared with state officials last September. Vermont authorities would not discuss the findings, but officials in California and Kentucky said this week that there was no evidence hackers succeeded in stealing anything.

Regulators said that given the number of weaknesses they discovered in just the three states studied, other state-run health insurance exchanges could be vulnerable, too. The GAO recommended the federal government continually monitor cybersecurity at such sites.

Created under President Barack Obama's health care overhaul, the exchanges are online marketplaces where people who have no health insurance through their jobs can buy government-subsidized private coverage. Only a dozen states ran their own websites this year; the rest either switched to the federal one or jointly operate their exchanges with Washington.

Computer security flaws are the just latest headache for the state exchanges. Some, like Oregon's, suffered crippling technical problems when they were launched in 2013. Some states, like Hawaii, turned operations back to the federal government because of cost concerns.

The GAO report examined the three states' systems from October 2013 to March 2015 and released an abbreviated, public version of its findings last month without identifying the states. On Thursday, the GAO revealed the states' names in response to a Freedom of Information request from the AP.

According to the GAO, one state did not encrypt passwords, potentially making it easy for hackers to gain access to individual accounts. One state did not properly use a filter to block hostile attempts to visit the website. And one state did not use the proper encryption on its servers, making it easier for hackers to get in. The report did not say which state had what problem.

Kentucky's Steve Beshear, who was governor when the security flaws were discovered, said through a spokeswoman that "because of the time required to fix the technical issues, not all those issues had been addressed" by the time Gov. Matt Bevin took office in early December. But Beshear added: "It is important to note that there were never any security breaches of any kind, and no one's information was ever compromised."

Doug Hogan, a spokesman for the Bevin administration's Cabinet for Health and Family Services, said efforts to fix the problems "are in various stages of completion and implementation." He added that privacy and security of sensitive information are "of the utmost importance" to Bevin's administration.

Kentucky's insurance exchange, kynect, will be dismantled later this year. While the system is credited with helping reduce Kentucky's uninsured rate from more than 20 percent in 2013 to 7.5 percent last year, Bevin says it is too expensive. He wants to transfer the more than 93,000 people who bought private coverage on kynect to the federal exchange, Healthcare.gov.

But Kentuckians' information might not be any safer on the federal exchange.

According to the GAO report, Healthcare.gov had 316 security incidents between October 2013 and March 2015. Such incidents can include

unauthorized access, disclosure of data or violations of security practices. None resulted in lost or stolen data, but the GAO said technical weaknesses with the federal system "will likely continue to jeopardize the confidentiality, integrity and availability of Healthcare.gov."

In Vermont, Lawrence Miller, director of health reform for Democratic Gov. Peter Shumlin, said the state had changed vendors since the period of the GAO review. During the transition, "we ensured the correct controls were in place" to meet a federal standard, he wrote in an email.

In California, a spokesman for the state's exchange, Roy Kennedy, would not say how Covered California was addressing the problems, citing security concerns. He pointed instead to a letter sent in October to members of Congress.

In its, Covered California Executive Director Peter Lee said there have been no successful breaches of website security. However, he said personal information may have been exposed in a few instances because of human error or other mistakes.

Lee said that Covered California adopted 37 of the GAO's 41 recommendations for improving security. He said his agency disagreed with three technical security recommendations and is constrained by state laws and union contracts from adopting a fourth—requiring background checks for existing employees.

Since the GAO audit, Lee's letter said, Covered California conducts more frequent scans to identify threats, and any critical findings will be immediately fixed.

"Protecting data is our highest priority," Lee wrote. "From day one, Covered California has followed the rigorous guidelines outlined in

federal and state security regulations designed to protect our consumers' private information."