Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Security Flaws Land ACA Contractors In Legal Crosshairs

By **Allison Grande**

Law360, New York (November 06, 2013, 10:16 PM ET) -- Security experts recently warned lawmakers that technical problems plaguing the Affordable Care Act's online insurance marketplace could expose vast amounts of personal data to theft, a worrisome report for contractors and government officials who handle that data and therefore risk becoming favorite targets for plaintiffs attorneys.

The first major indication that the insurance exchanges might not be capable of protecting the troves of sensitive consumer data fed into them came in August, when the inspector general of the U.S. Department of Health and Human Services reported that the federal government had missed several deadlines to test the system for vulnerabilities and implement safeguards.

The report prompted Sen. Orrin Hatch, R-Utah, and others to push legislation that would delay the launch of the exchanges until the government could ensure they had strong protections. But the Internet-based hubs opened for business as scheduled Oct. 1, and their operators have done little in the past month to dispel privacy concerns, according to attorneys.

“We don't have the information yet to know whether or not the data security risks are real or worse than expected or have been fixed, so our assessment of the privacy risks associated with having so much incredibly sensitive information passing through these systems has not changed since they went live,” said Cynthia Larose, the privacy and security practice chair for Mintz Levin Cohn Ferris Glovsky & Popeo PC.

Given the sensitivity of the information consumers and federal agencies must put into the system to determine coverage eligibility, experts predict that the probability of a data loss that could expose the controllers of the information to liability is high.

“By combining so many federal databases and feeding in additional financial, health and other data from consumers reportedly without encryption or other safeguards, you're creating a huge honey pot for nation-states and other potential hackers,” said Brian Dean, the audit and compliance manager at information security management consulting firm SecureState. “That creates legal ramifications, since there are laws on the books today with regard to data breaches.”

While the federal privacy laws that govern the handling of health and financial data do not have a private right of action, consumers could seize on state data breach and privacy laws to bring suits against government entities or contractors that fail to protect their data in these exchanges, attorneys say.

“I'm sure that in the event of a breach, plaintiffs lawyers will try to employ theories that enable them to make claims under state privacy laws or similar theories,” said O'Melveny & Myers LLP health care and life sciences practice co-chair Michael Maddigan.

However, attorneys pointed out that consumers might face an uphill battle in pursuing their claims, given the hurdles plaintiffs have traditionally faced in proving that a loss of sensitive data caused them actual harm.

“It's been notoriously hard for plaintiffs in data security class actions to maintain their claims, so unless the private cause of action is related to certain information that was compromised, it would be pretty difficult to initiate an action for a breach of the system,” Larose said.

Plaintiffs might also have difficulty pinning liability for the data loss on a responsible entity in the vast web of the exchanges, according to attorneys.

“There are patients, payers, providers, employers, the government, vendors, and subcontractors to the vendor accessing this information, and many of these entities have complex relationships and contracts that may limit their exposure,” said Kilpatrick Townsend & Stockton LLP health care, life sciences and technology co-chair Sidney Welch.

Still, government agencies and contractors that fail to protect the data stored in the exchanges could also face backlash from HHS, the Federal Trade Commission or state attorneys general, who have been active in warning consumers about scams associated with the new marketplace.

For example, any entity that violates the rule that personally identifiable information may not be used or disclosed to an insurance exchange except to carry out its functions could be subjected to a civil penalty of $25,000, Morgan Lewis & Bockius LLP partner W. Reece Hirsch pointed out.

A breach could also be reported to and investigated by the Office of Civil Rights if the party responsible for the data is a covered entity or business associate under the Health Insurance Portability and Accountability Act, according to Welch.

However, some attorneys doubted whether federal and state enforcers would pursue data security violations very aggressively, given their close ties with the exchanges.

“The question becomes, who regulates the regulator?” Larose said.

Despite potential difficulties, plaintiffs and enforcers are unlikely to abandon the issue anytime soon, according to attorneys — and a pair of recent developments illustrate the continuing interest in the topic.

First, a North Carolina man reported Friday that he had been given access to the records of a South Carolina attorney through an insurance exchange. The disclosure came one day after Gartner Research Vice President Avivah Litan wrote an Oct. 31 blog post that highlighted many of the security concerns with the exchanges and called on the Obama administration to take down the site indefinitely to institute the proper layers of defense, said Kilpatrick Townsend partner Jon Neiditz.

The information mix-up revealed Friday comes on the heels of a September report that an employee of Minnesota's then-inactive exchange had mistakenly shared a document containing the personal information of 2,400 insurance agents and brokers that applied for certification with the database.

But despite the panic, experts noted that the contractors and government entities that make the exchanges run could improve the security of the systems — and reduce their liability — by instituting several common security safeguards, such as encrypting data and minimizing the amount of data necessary to participate in the exchange.

“As long as they're using secure solutions at the back end, that's what's going to prevent or lower the risk of the hacking of the website or the content stored behind it,” said Rama Kolappan, the director of product marketing for secure mobile file sharing provider Accellion.

While some of the entities that are involved with the exchanges may be unfamiliar with these protections, many of the contractors involved with the exchanges already have procedures in place for protecting sensitive information, attorneys pointed out.

"Will breaches and improper disclosures happen as part of the new federal and state exchanges? I wouldn’t bet against it,” said Foley Hoag LLP privacy and data security practice co-chair Colin Zick. “But it’s not a new world — just an expansion of the existing one.”

--Editing by Kat Laskowski and Chris Yates.