Hackers access records for millions of Anthem customers

Posted: Feb 05, 2015 11:45 Updated: Feb 05, 2015 11:45 AM

INDIANAPOLIS (AP) - Hackers broke into a health insurance database storing information for about 80 million people in an attack bound to stoke fears many Americans have about the privacy of their most sensitive information.

Anthem, the nation's second-largest health insurer, said it has yet to find any evidence that medical information like insurance claims or test results was targeted or taken in a "very sophisticated" cyberattack that it discovered last week. It also said credit card information wasn't compromised, either.

The hackers did gain access to names, birthdates, email address, employment details, Social Security numbers, incomes and street addresses of people who are currently covered or have had coverage in the past.

An Anthem spokeswoman said Thursday the insurer was working with federal investigators to figure out who was behind the attack. They had not pinned down the exact number of people affected.

Anthem Inc., which recently changed its name from WellPoint, runs Blue Cross Blue Shield plans in more than a dozen states, including California, New York and Ohio. It covers more than 37 million people.

Cybersecurity experts say these hackers may not be done with the insurer, and health records are becoming more attractive to them, as previous targets like the retailers Target and Home Depot shore up their defenses.

"To me, this is the next wave of where were going to see more and more attacks," said Mark Bower, a vice president with the cybersecurity firm Voltage Security. "Cybercrime is a business. The attackers will simply move to the next low-hanging fruit."

He said security practices in health care are not as mature as they are in other industries, and hackers have multiple ways to get into a health care system that links insurers, care providers, labs and other businesses that handle sensitive patient information.

Medical records can be sold to criminals who could construct billing and insurance scams involving fake medical centers or target patients for phone scams.

"That's the kind of sophistication we have in cybercrime," Bower said. "We have networks of criminals who can use this data whenever its available based on their skill set."

Medical data also can be used to extort patients, with the hacker demanding money to prevent the public release of sensitive information, said Eran Barak, CEO of another cybersecurity firm, Hexadite.

He added that the attack may have been a probe to test the insurer's defenses, with hackers planning to return for more

information or installing malware that steals data.

The insurer said all of its product lines were affected. It sells mainly private individual and group health insurance, plans on the health care overhaul's public insurance exchanges and Medicare and Medicaid coverage. It also offers life insurance and dental and vision coverage.

Affected brands include Anthem Blue Cross, Blue Cross and Blue Shield of Georgia, Empire Blue Cross and Blue Shield and Amerigroup.

This wasn't Anthem's first security breach.

In 2013, the insurer agreed to pay $1.7 million to resolve allegations it left the information of more than 612,000 members available online because of inadequate safeguards. The U.S. Department of Health and Human Services said that security weaknesses in an online application database left names, birthdates, addresses, telephone numbers, Social Security numbers, and health data accessible to unauthorized users.

The Health and Human Services Department said then that the insurer didn't have adequate policies for authorizing access to the database, didn't perform a needed technical evaluation after a software upgrade, and did not have technical safeguards to verify that the people or entities seeking access were authorized to view the information in the database.

In 2008, the insurer offered free credit monitoring after it said personal information for about 128,000 customers in several states had been exposed online. In 2006, backup computer tapes containing the personal information of 200,000 of its members were stolen from a Massachusetts vendor's office.

CEO Joseph Swedish, who was not running the company when those security breaches occurred, apologized to customers on a website that the insurer established to explain the latest problem, **www.anthemfacts.com**.

"We will continue to do everything in our power to make our systems and security processes better and more secure, and hope that we can earn back your trust and confidence in Anthem," he said.