Anthem discloses largest ever health care industry cyber attack

February 6, 2015

Anthem, Inc., one of the nation's largest health insurers, disclosed on Wednesday that hackers had gained access to a database containing the personal information of 80 million current and former members and Anthem employees. The attack, which was first reported by The Wall Street Journal, is the largest ever in the health care industry and ranks among the largest in any sector.

Anthem is currently conducting an investigation into the scope of the breach, and the F.B.I. has launched a parallel investigation. While Anthem reported that credit card numbers and member claims data was not compromised, the hackers did have access to names, Social Security numbers, addresses, dates of birth, employment information and income data.

Anthem sent an email to current members early Thursday morning, stating: "Once the hack was discovered, Anthem immediately made every effort to close the security vulnerability, contacted the F.B.I. and began fully cooperating with their investigation." In addition, the email stated that Anthem has retained a cybersecurity firm to evaluate its systems and identify solutions to the vulnerabilities.

This is the second large-scale hack on a health care entity to occur recently, after hackers used the "Heartbleed" security flaw to steal approximately 4.5 million patient records from Community Health Systems last year. Shortly thereafter, in April 2014, the F.B.I. issued a Private Industry Notification warning that "the health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely." The F.B.I. Notification cited reports stating that "health care security strategies and practices are poorly protected and ill-equipped to handle new cyber threats exposing patient medical records, billing and payment organizations, and intellectual property."

The Anthem news reinforces the warnings from the F.B.I. and highlights the critical importance of strong electronic security measures for all businesses and, in particular, all HIPAA covered entities and business associates. After security measures are implemented, they should be tested and reevaluated on a regular basis in order to keep pace with hackers, whose methods are constantly evolving.

Authors

Chris Bennington

Partner

Cincinnati
513.870.6572
cbennington@bricker.com