More than 18,000 members affected by Anthem's second major data breach

DATA PRIVACY SOLUTIONS | AUG 01, 2017

Anthem is reporting their second major data breach in two years, this time with approximately 18,500 members' information at risk after a third-party vendor's employee emailed a file with member records to himself.

According to a statement released by the insurance provider, that third party, LaunchPoint Ventures – which provides insurance coordination services to Anthem – said that it learned of the breach after one of its employees was involved in "identity theft-related activities" on April 12, 2017. Following this incident, LaunchPoint hired a forensics firm to further investigate the issue, which revealed the employee's emails. On May 28, 2017, LaunchPoint learned that the employee had misused another company's data as well as having emailed a file with information about Anthem companies' members to his personal email address on July 8, 2016. The LaunchPoint employee has since been fired and arrested, but on charges unrelated to this case, according to Anthem.

On June 12, 2017, LaunchPoint confirmed that the file in question included the protected health information (PHI) of Anthem members and reported the incident to Anthem two days later. Anthem reported the breach to the Department of Health and Human Services, Office for Civil Rights on July 24, 2017.

WHAT ANTHEM MEMBER INFORMATION IS AT RISK?

The PHI within the file included more than 18,500 Anthem members' Social Security numbers, Health Plan ID numbers, Medicare contract numbers, ID numbers and dates of enrollments, and in some cases, last names and dates of birth were also included.

This breach comes on the heels of a landmark settlement reached last month to resolve a class action lawsuit brought against Anthem in which the health insurer agreed to pay $115 million over a 2015 data breach that affected the personal information of nearly 80 million customers.

INSIDER THREATS AND THIRD-PARTY PROVIDER RISKS

Data shows that insider threats still make up a large portion of data breach incidents and healthcare executives see employee security awareness and culture as their number one threat. At the same time, payer and providers favor funding for cybersecurity technology over staff hiring and training. Though the payer could have stringent cybersecurity policies and data best practices in place, it cannot always control the actions of the third-party providers. But, the problem remains that companies cannot dispense with the third-party ecosystem. Organizations need external providers to help keep systems running, whether that's building service providers or insurance coordination services.