New Healthcare Data Breach Involves 10.5 Million Insurance Customers

September 16, 2015 - Excellus BlueCross BlueShield, which is based in New York, has released a statement indicating that the companyâ€™s computer system was hacked; resulting in a data breach for 10.5 million of the companyâ€™s customers Breached data includes names, addresses, birth dates and social security numbers.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

The breach went undetected by the company for more than a year and a half. The company believes that it began in December of 2013 but it wasnâ€™t detected until the beginning of August this year.

The breach is just the latest in a series of hacking incidents targeting healthcare providers and insurance companies. The largest breach in this sector so far â€“ potentially exposing more than 80 million people - involved Anthem, Inc.

ACCESS expects hackers to continue to target this market segment for a variety of reasons. First, the data obtained from insurance companies can be sold for both financial and medical identity theft. This increases its value on the black market. Second, many insurers have access to huge databases. Hackers gaining access to these databases can reap almost unimaginable rewards. And finally, the healthcare industry as a whole is behind the curve on data security and the hackers know this.

Anyone who thinks that their data may have been compromised needs to be looking at their credit reports regularly and may want to consider using an identity theft prevention service. Additionally, victims will need to closely monitor any correspondence from their insurance company. Specifically, they need to be checking any statements detailing medical treatment to make sure that it is accurate. Inaccuracies caused by medical identity theft can have a greater impact on

victims than those caused by financial identity theft. Not only can they be expensive in terms of dollars, but they can lead to misdiagnosis, inaccurate treatment and potential injury or death.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS