Horizon Blue Cross Blue Shield Announced Data Breach Affecting 840,000 Customers

December 11, 2013 - Two laptop computers belonging to Horizon Blue Cross Blue Shield were stolen from a company facility in Newark, NJ at the beginning of November. The computers, which were affixed to the desks they were on with locks, contained unencrypted data on 840,000 Horizon customers in New Jersey.

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 theft was reported to police on November 4th. The data contained on the computers included customer names, addresses, social security numbers, Horizon account numbers, dates of birth and some patient clinical information. This is more than enough data for anyone with access to it to commit both financial and medical identity theft.

An announcement released by Horizon reads, "We have no reason to believe that the laptops were stolen for the information they contained or that the information has been accessed or used in any way. However, in an abundance of caution, we began sending letters to affected members on December 6, 2013."

"Horizon BCBSNJ has also established a dedicated call center for members to contact with any questions. If you believe you are affected but have not received a letter by December 20, 2013, please call 877-237-9502 Monday through Friday between 9:00 a.m. and 7:00 p.m. Eastern Time (closed on U.S. observed holidays), and provide the following ten digit reference number 2156112613 when prompted."

There is no excuse for storing unencrypted highly personal customer data on computers yet many companies continue to do so. This particular case is especially disturbing since it isn't the first major data breach involving the company's customer data. According to a report by HealthITSecurity, the company had a similar issue in 2008 when a computer with data on 300,000 customers went missing.

Horizon is offering those affected in this latest incident one year of free credit monitoring. As always, ACCESS position on credit monitoring is that it is a useless service; only notifying you after you have been victimized.

Anyone who has reason to believe that their information may have been exposed in this breach would be well advised to place a freeze on their credit file.

Unfortunately, there is no similar mechanism available to freeze one's medical file. That's a big issue because the

Affordable Care Act mandates the use of electronic medical files. Anyone whose data is used to commit medical identity theft could find that their medical files contain inaccurate information. In some cases - say, for people who are allergic to certain medicines - medical file inaccuracies could result in serious complications or even death.

Anyone experiencing medical ID theft as a result of this breach needs to closely monitor all communications and claims documents issued by their insurer. Any claims that are not recognized should be disputed immediately. Not doing so could result in increased insurance premiums and even legal fees. Additionally, medical ID theft victims need to maintain paper copies of their medical records. When seeking any form of treatment, victims should insist on reviewing the doctor's medical records if those records are stored electronically. Not doing so could result in misdiagnosis, injury or even 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