AHMC Healthcare Data Breach Exposes 729,000 People for Potential ID Theft

October 22, 2013 - The theft of two laptop computers from a guarded AHMC Healthcare facility has exposed the personally identifiable information of 729,000 people; potentially setting them up for fraud and ID theft. While the computers were password protected, the data stored on them was apparently not encrypted.

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 facility where the computers were located was guarded, gated and used video surveillance. But that wasn't enough to stop the thieves who broke into an office and took them on October 12th.

The records contained on the computer hard drives were for Medicare patients and contained Medicare/Insurance ID numbers, diagnostic codes and payment information. Approximately 10% of the records also contained patient Social Security numbers.

While the SSN information and other data may be used for traditional identity theft, the stolen insurance information could be even more problematic as it can potentially be used to commit medical identity theft. Under the new healthcare law, doctors and hospitals are being forced to convert to electronic medical records. Because of this, doctors around the country will be able to access anyone's medical records in an emergency. But anyone who has been the subject of medical identity theft could find that their records contain inaccurate information; something that could lead to potentially fatal treatment decisions.

In cases of traditional identity theft, consumers have the ability to place a freeze on their credit file. But in cases of medical ID theft, there is no ability to freeze your medical file and there is no provision within the new law that even

contemplates a record freeze.

This particular theft took place in California and affects patients who received treatment at Garfield Medical Center, Monterey Park Hospital, Greater El Monte Community Hospital, Whittier Hospital Medical Center, San Gabriel Valley Medical Center and Anaheim Regional Medical Center. While we expect most potential victims to reside in California, any Medicare patients treated at any one of these facilities in the past should be concerned regardless of where they currently reside. Anyone who is concerned that their information may have been included in the breach can contact AHMC at (855) 977-6678.

The company has stated that it believes the risks of the stolen data being used for ID theft are low but ACCESS doesn't agree with that assessment. Even though the stolen computers were password protected, bypassing password security is fairly simple for anyone with moderate computer skills and a little patience. If the thieves know about the stolen information, and if they believe it has value, in our estimation it is probably only a matter of time before they attempt to sell it or begin using it themselves.

Anyone who is able to confirm with AHMC that their information was included in this breach should seriously consider placing a freeze on their credit file. Additionally, medical bills and insurance payment information will need to be closely watched for the rest of their lives. Any medical charges or payments made for unrecognized services need to be challenged immediately.
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