Three Big Medical Data Breaches Finish Off 2011

December 15, 2011 - As the year rolls to a close, the number of people targeted for medical identity theft continues to rise. That's not really surprising when you consider that the cost for medical insurance increased significantly in 2011. Those price increases make the personally identifiable information of those with health insurance much more valuable. So it is no wonder that three of the largest data breaches in the last half of this year involve healthcare information.

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);
})();

Medical ID theft isn't quite the same as ID theft involving credit. In the first place, if your medical identity is stolen, you can't call the FTC or the credit bureaus and have them freeze your records. That means cleaning up the theft of your medical information could be significantly more difficult (and for anyone who has been the victim of traditional ID theft, that is saying something), or even impossible.

In the second place, the information required for medical ID theft is a little different. Specifically, in addition to all of the traditional information needed for identity theft, the crooks also want to get their hands on your insurance policy information.

The three data breaches mentioned above were caused by a variety of factors including negligence, lack of security and stupidity.

In one, a company by the name of Nemours managed to leave data tapes in a file cabinet that went missing during a building remodel. Those tapes included bank account numbers, SSNs, names, dates of birth and insurance data for 1.6 million people. This particular case sounds more like negligence than anything else. At least, that's my opinion.

Then there is the case of Sutter Physicians Services and Sutter Medical Foundation. Here, a resourceful thief broke into Sutter's offices and stole a computer with the personally identifiable information of more than 4 million people. Out of those records, nearly 950,000 of them included medical information. And "no", the computer's data was not encrypted. Again, just my opinion but this one is a combination of all three of the causes previously mentioned. It is worth noting that Sutter is also being sued for negligence as a result of the theft.

And finally, there is the case of Tricare - A US Government owned agency. The primary apparent cause of this beach looks like stupidity, closely followed by a lack of data security. One of the company's subcontractors had an employee who was driving around with a computer tape containing patient data in the back of his car. The tape was stolen. It was not encrypted. And it contained the data on more than 5 million patients who had visited military hospitals between 1992 and 2011.

The three breaches account for nearly 11 million individual records. And unfortunately, the data stolen can be used for both medical and traditional ID theft.

Corporations and government agencies have known for years that storing personally identifiable information in unencrypted records leads to data breaches. They also know that when data is being transported outside of the confines of what are supposedly secure offices, encryption is all the more important.

The fact that the federal government was responsible for roughly half of these breaches is all the more disturbing when you consider the fact that the department of Health and Human Services is attempting to mandate that all medical records be stored electronically.

Anyone who believes that their information may have been leaked in one of these breaches needs to call the credit reporting agencies and place a fraud alert on their credit file. If access to immediate credit is not important to you, then you should seriously consider placing a freeze on your credit file.

Additionally, anyone who believes that their information may have been exposed in one of these breaches needs to closely monitor any insurance notices that they receive. You may want to consider notifying your insurance carrier and asking to have your policy number changed. Additionally, if possible you may want to add a security password or PIN to your account if your provider will let you. At least that will make it more difficult for anyone else to access funds from your insurance company.

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: