Cancer Patient Data Released in Medical Record Data Breach

June 29, 2012 - My dad used to say, "Life isn't fair. Get used to it." He was right, and what happened to thousands of patients at M. D. Anderson Cancer Center at the University of Texas proves it. Their personal data was on a computer that was stolen. And like many data breaches, this one never should have happened in the first place.

According to the June 28th Houston Business Journal, the computer theft could affect as many as 30,000 M. D. Anderson patients. And the data contained on the computer is enough to commit both financial and medical identity theft. According to various reports, including a statement from the university, the data included names, addresses, medical record numbers, social security numbers and other highly personal information.

As bad as all of this is, it isn't the entire story. In fact, this really isn't a story about just a single data breach. It is a story about companies and organizations that continually fail to implement sound data security policies.

In this particular case, a doctor at M. D. Anderson had the data stored on a laptop computer. The data was not encrypted, so anyone who has access to the computer can look at it. And he brought the computer home with him, only to have it stolen.

If that sounds like a familiar story, that's because it is. Several years ago, an analyst for the Veterans Administration brought home a computer with similar unencrypted data on roughly 23 Million people. That analyst's house was also burgled and the computer was stolen. People across the country were screaming bloody murder over the incident and many organizations did take action to protect their customer and employee data. But that less was lost on many others; apparently including M. D. Anderson.

In ACCESS opinion, there is simply no excuse for this particular type of data breach. It wasn't caused by hackers. It wasn't caused by a new computer virus. Its cause was a well known human error that never should have been allowed to happen.

Every organization that works with the personally identifiable information of clients or employees has a responsibility to protect that information. They can start by encrypting their data. There are numerous encryption programs available and many of them don't cost a penny. They can also protect data by having data security policies in place that forbid the use of this type of data off of their premises. If they absolutely need to be able to use data in remote locations, then they need

to insure that they have additional policies and programs in place to protect it. Developing such policies isn't rocket science. It is just common sense.

M. D. Anderson is currently in the process of notifying those who were impacted by this breach. Since the burglary involved the theft of multiple items - not just the computer - it is doubtful that the thieves were targeting the data stored on the computer. But it is impossible to know if they will find the file with the data in it, and if they do, if they will use it.

Anderson is offering victims one year of credit monitoring service - something which we have repeatedly said is useless because credit monitoring only notifies you once you have become an ID theft victim. They have also setup a hotline for inquiries. If you have any reason to believe that your data may have been included in this breach, you can reach them at 1-877-441-3007, Monday through Friday, from 8:00 AM to 8:00 PM Central Time.

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