Kaiser Permanente Data Breach Involved Missing Flash-Drive

December 13, 2013 - The latest healthcare data breach isn't large by current standards. The breach affects 49,000 patients at the Kaiser Nuclear Medicine facility in Anaheim, CA. Yet the relatively small number of patients impacted is worth noting because it illustrates just how easily information can disappear with some assistance from modern technology. No need for anyone to steal a computer. Just plug in a flash drive and slip it back into your pocket when nobody else is looking.

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 Kaiser data breach may not have been a theft. Based on the scant amount of information revealed by Kaiser, it could be a simple matter of someone misplacing a flash drive; a small device about the size of a key.

What is known about the breach is that the names, dates of birth, Kaiser medical record number and treatment information were stored on the missing drive. Kaiser has also said that the information was unencrypted - meaning that anyone with access to the drive can open the files contained on it.

The breach probably doesn't provide anyone with enough information to commit traditional identity theft. Social security numbers were not included. But Kaiser clearly believes that it may provide enough information to commit medical ID theft. The company is warning affected customers that they should carefully monitor their medical files for accuracy. They do not however suggest a way for their clients to do that on a long term basis.

There has been a recent increase in the number of medical data breaches and there are now a wide variety of studies which show that the medical industry is not doing enough to protect patient data. It has become increasingly easy and convenient for doctors, hospitals and healthcare workers to upload large amounts of patient data on portable computing devices and smart phones. But the medical industry has been particularly slow in implementing strong data protection policies.

Even simple steps such as encrypting stored information could prevent a large number of medical data breaches. But the industry has largely ignored calls by privacy advocates to implement new protection procedures. Until this attitude changes, we can expect to see more and more data breaches of the type described here.
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