# Medical Data Breaches Expected To Rise Over Coming Year

January 13, 2012 - According to a report by ID Experts, a company that markets data breach services to corporations, medical data breaches are increasingly difficult to prevent. The report named 11 trends taking place within the industry to manage medical data. Several of these trends indicate that troubling times lie ahead for consumer privacy and identity theft.

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);
})();

According to the IDE report, the proliferation of mobile devices is one of the key reasons that we can expect to see explosive growth in medical data breaches. But it is not just the devices themselves and the fact that they are often carried about by employees in unsecure locations that pose the threat. It is also the fact that about half of companies dealing with medical data don't appear to be doing anything to secure that data.

The report cites data from another report conducted by the Ponemon Institute. Of the companies surveyed by Ponemon, 81% of respondents stated they were using mobile devices to gather and store sensitive data. But only 51% of those companies were doing anything to secure the data stored on the mobile devices they use.

According to IDE, they also expect that the use of mobile devices will explode over the coming year; exacerbating the problem further.

Another issue covered by IDE is the increased use of outsourcing by companies managing medical records. When companies, such as insurers and hospitals outsource functions that deal with patient data, they effectively lose control of that data, the way it is stored, who has access to it and any security measures used to safeguard it. In some instances,

records may actually be handled outside of the United States. This means that American privacy laws may not longer be applicable.

IDE also cites the growth of cloud computing as a potential issue related to data breaches. In cloud computing, data may be managed in several locations but is stored off-site. This often involves the use of leased computing facilities that may not be under the direct control of those who are responsible for managing patient record.

While cloud computing does offer businesses certain benefits in terms of cost and flexibility, it also increase privacy risks because all data is stored and made available via a network connection. This usually means an internet connection.

Medical data breaches can be especially devastating to victims because medical records contain a wide variety of personal information. The data can be used for both traditional identity theft and to receive medical treatment (known as medical ID theft).

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