VA Putting Veterans at Risk for ID Theft and Fraud - Violating Federal Regulations

March 12, 2013 - In May, 2006, the Department of Veterans Affairs (VA) had a computer stolen which contained the names, addresses, SSNs, birth dates and other highly sensitive data on 26.5 million people. The data included veterans, some of their dependents and some active duty military personnel. All of the data was unencrypted, and it was walked out of the VA on a laptop computer by a consultant who was subsequently robbed. The breach led to a variety of new regulations on the storage and transmission of this type of data. Regulations which - of all agencies - the VA has apparently decided to ignore.

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);
 })();
```

A report by the VA's Inspector General (OIG) has determined that the agency has broken federal regulations on data encryption and transmission. The report determined that the agency has regularly been transmitting unencrypted highly sensitive, personally identifiable information belonging to veterans between certain facilities.

Perhaps even more disturbing is the fact that these transmissions were not a mistake. Upper management at the VA signed off on waivers which allowed these transmissions. Those waivers apparently violated federal law.

According to the VA, the data was not transmitted over the internet. Instead, it was transmitted across the VA's network. But those network lines are not actually the property of the VA. The lines are supplied by various regional and national telecommunications providers outside of the VA's control. The report acknowledges this and states that this type of transmission can be compromised and could jeopardize the entire VA network. OIG investigators are concerned that hackers could learn enough about how the VA's network functions that they could then steal more information and even take the entire network down.

This particular blunder took place in the Midwest and impacts veterans in Iowa, Minnesota, Nebraska, North Dakota, South Dakota and parts of Illinois, Kansas, Missouri, Wisconsin, and Wyoming. The overall size of the violation is unknown at this time. It was discovered during investigations of medical facilities in Nebraska and South Dakota, but investigators believe that it could be much larger.

It is very clear that the VA has not learned from its prior experiences. But what's really frightening is that the government is now pushing insurance providers and doctors to move to electronic medical records for all of us. If this breach is any indication of what is to come, we are all in for a very rough 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