FBI Issues Warning that Healthcare Records Are Now at Increased Risk of Being Hacked

May 7, 2014 - The FBI's Cyber Division has issued a warning to healthcare providers that their records are at increased risk for hacking and being used to commit medical identity theft. The warning places the primary blame for this on the mandatory conversion from paper to electronic medical records which was codified into law as a part of the Affordable Care Act, and a lack of technical preparedness within the industry itself.

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);
})();
```

By law, medical records must be converted to electronic form by January 1, 2015. But according to reports from " SANS, Ponemon, and EMCÂ²/RSA, the health care industry is not technically prepared to combat against cyber criminalsâ€™ basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs)."

The warning memo goes on to say that a variety of medical devices used in hospitals and other facilities appear to be particularly vulnerable to attack. Yet those in charge of cyber-security in these facilities appear to be in denial of this. "The biggest vulnerability was the perception of IT health care professionalsâ€™ beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise."

Additionally the memo state, "According to a Ponemon Institute report dated March 2013, 63% of the health care organizations surveyed reported a data breach in the past two years with an average monetary loss of $2.4 million per data breach. The majority of each data breach resulted in the theft of information assets. Lastly, 45% reported that their organizations have not implemented security measures to protect patient information.

The conversion to electronic medical records was one of the very first items that ACCESS protested in the Affordable Care Act, for this very reason. It was apparent that the conversion to electronic records would necessitate the formation of huge consumer databases which would become almost irresistible targets for hackers and identity thieves. Those predictions are now coming to fruition.

Unfortunately, there are currently no federal or state laws which would allow consumers to freeze their medical records in much the same way that they can freeze their credit file. This is a significant problem which is likely to result in permanent injury or even death for some victims of medical ID theft. Once your medical record has been stolen and used by someone else, it may contain incorrect information such as incorrect drug allergies.

Congress needs to take a serious look at this issue and adopt a set of regulations that give consumers final control over their medical information. And they need to take action before there is a tragedy reported in the media.
 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