First Obamacare Data Breach Reportedâ€¦ Well, That Didn't Take Long!

October 2, 2013 - We've been warning our readers for two years about the potential for data breaches and identity theft victimization as a result of massive consumer databases being built for Obamacare. But even we didn't think that the first breach would occur within hours of the time that people could start the healthcare registration process under the new law. But that's precisely what happened.

The Affordable Care Act (ACA), commonly referred to as Obamacare, is heavily reliant on the construction of consumer databases. The law is forcing doctors and hospitals to convert to electronic medical records. This move will allow those records to be easily shared among healthcare providers. It also provides an attractive repository of vulnerable consumer data for fraudsters and ID thieves.

Additionally, the law mandates the establishment of healthcare exchanges where consumers can purchase insurance policies. These exchanges require the consumer to reveal social security numbers, tax documentation, birth dates, etcâ€¦ Everything an ID thief needs to operate.

Working hand in hand with the healthcare exchanges are people who are known as "navigators". We've previously written about navigators and the roll we expect them to play in identity theft but here is a quick refresher. Navigators don't work for the government or the exchanges. They are contract players, often with nonprofits. They are responsible for gathering all of your personally identifiable information - including your SSN - and getting you enrolled in a plan. And the government doesn't require them to go through any background checks at all.

The bottom line here is that it has never been a matter of "if" there would be data breaches or ID theft associated with the ACA, but a matter of when. And the "when" (at least with regard to a data breach) occurred yesterday; the very first day that the healthcare exchanges were opened for business.

Yesterday's event was relatively small. It occurred on the Minnesota healthcare exchange, MNsure.com.

An employee at MNsure was sending an email message to two insurance agents. That employee attached a file containing the names, addresses and SSN's of 2,400 people to the message. Once the incident was discovered, the two people that the message was sent to were asked by the exchange to delete the file. After that, MNsure began notifying those whose names were contained in the file that their data had been breached.

While this particular incident probably won't lead to ID theft, it also shows just how lacking the data security standards are for these new healthcare exchanges. The chances are pretty good that yesterday's data breach was small simply because it happened on the first day that the exchange was open. It could have been much larger if more people were enrolled.

This is the first of what we expect will be many more data breaches over the next few months. If the government is going to force consumers to turn over their most private data and have it warehoused in electronic databases, then it has an obligation to provide reasonable security standards to protect that data. It is very clear that, at least right now, that's not happening.

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