

OPENING STATEMENT

Hon. Eddie Bernice Johnson, Ranking Member
Committee on Science, Space & Technology
Full Committee Hearing:
“Is My Data on Healthcare.gov Secure?”

Tuesday, November 19, 2013 at 10:00 a.m. in Rayburn HOB 2318

Good morning, and welcome to our witnesses. I look forward to your testimony.

In light of the startup problems that have been reported with the Healthcare.gov website—problems that need to get fixed as quickly as possible—some Americans may be concerned about the security of their personal information on the website. I can understand such concerns, because anytime any of us go on the internet, we are vulnerable to those who would attack public and private databases to get access to our information.

That said, we have not heard much about security failures at Healthcare.gov. There is one recorded instance where an individual was mistakenly given access to the records of another person. There were initially security issues with the password reset function. The site has also been attacked by hackers in a “denial of service” attack. However, my understanding is that these issues were quickly fixed and the cyber-attack was successfully prevented.

The reality is that Healthcare.gov is subject to the same attacks as every other website and every other internet-accessible data base. Every Member of this Committee knows that computer vulnerabilities are exploited every day at companies and government offices across the world, leading to the compromise of a wide range of personally sensitive information.

I would like to draw your attention to a graphic that tries to illustrate major security failures of computer systems resulting in personal information being compromised.

As you can see, some of the biggest and most experienced internet firms have suffered attacks--and often the personal information that is accessed goes well beyond identifying information to include credit card and sensitive financial information. Governmental institutions have also seen materials stolen.

Last year, Symantec’s annual 2012 Cybercrime Report, found that 556 million individuals in 24 countries, including the United States, were victims of one sort of consumer cybercrime or another. This equates to 1.5 million victims every day.

One might conclude that the only way to avoid being vulnerable to such attacks is to not be connected to the internet at all. However, in the 21st century that is not a reasonable option for most government agencies, businesses or individuals. So, I think we have to be realistic about the ability of any internet-connected database to be completely invulnerable to being compromised.

I also think we have to be honest about what information actually will be available to a cyber-attacker through Healthcare.gov. In my work as a psychiatric nurse I saw how patients' medical records were routinely accessed by large numbers of people every day. Several years ago my own electronic medical records were breached and I received a letter informing me about this from the hospital in Dallas.

So how vulnerable are our medical records on Healthcare.gov? Some, including two of the witnesses invited to testify today, have made public claims that the website will have all kinds of sensitive personal medical records in its database. That is simply not true.

Healthcare.gov will not have patient or healthcare case information about anyone. Healthcare.gov will have the name, date of birth, social security number and address of participants, but that information is also potentially available through every insurance company, bank, credit card company and government agency that anyone deals with, and I've already pointed out the data breaches that have occurred and are occurring in those sectors of our economy.

So while there can be legitimate concerns about privacy in the health care field, Healthcare.gov should not be the cause of any exceptional fears in that regard. By saying that, I am not excusing the startup failures to implement the ACA website in an effective way, nor am I saying security failures are acceptable. They are not. I expect HHS will take every measure available to them to make the site secure and to maintain a high level of security going forward. However, I want everyone to keep the issues of security in perspective, and I hope that none of us will use this hearing to engage in fear-mongering in an effort to destroy participation in the ACA. That would be irresponsible and, frankly, cruel. The Americans who most need the ACA to work are those that are among the most vulnerable members of our society.

Their personal medical data is not at risk on Healthcare.gov. In fact, it can be argued that this Committee's efforts to force sensitive information out of EPA, Harvard, and the American Cancer Society are a bigger threat to patient privacy than is Healthcare.gov.

In closing, I hope that today's hearing will not become a soap box for sowing fear and confusion. Let's stay focused on the facts.

With that, I again want to welcome our witnesses, and I yield back the balance of my time.