For Immediate Release
February 12, 2015

Media Contacts: Zachary Kurz, Laura Crist
(202) 225-6371

Statement of Research and Technology Subcommittee Chairwoman Barbara Comstock (R-Va.)
Can Americans Trust the Privacy and Security of their Information on HealthCare.gov?

Chairwoman Comstock: Three weeks ago, on January 20, the Associated Press reported that as many as 50 data mining companies had access to consumers' personal and health information on HealthCare.gov. Companies such as Google, Twitter, Facebook, Yahoo, and Advertising.com apparently were provided access by CMS (the Centers for Medicare and Medicaid Services).

As reported by AP, "When you apply for coverage on HealthCare.gov, dozens of data companies may be able to tell that you are on the site." While the information shared with these third party companies does not include the health care consumer's Social Security number, it appears that a number of data companies may have had access to consumers' age, income, ZIP code, smoking practices, pregnancy status, and even computer IP address.

While some may characterize this as a harmless collection of data, it can actually be much more revealing. A recent MIT study of credit card data revealed that only four pieces of outside information about a user, including one's social media activity, were sufficient to identify a person in the database of a million people.

The concerns with HealthCare.gov's practice of sharing data with companies like Google, Twitter and Facebook are two-fold. There are privacy implications of feeding consumers' personal data -- unbeknownst to them -- to third party vendors, and there are security concerns, because additional connections to the website can lead to additional vulnerabilities.

We also should consider this news in the context of President Obama's announcement that he would bring forward a new online privacy and cybersecurity proposal later this month. This proposal was described as building on steps previously taken to "protect American companies, consumers, and infrastructure from cyber threats, while safeguarding privacy and civil liberties." It seems to me that what the AP has reported about Americans' data on HealthCare.gov and what the President expects of Americans may be in conflict or certainly raise legitimate concerns.

Privacy protections at federal government websites should be the gold standard, setting the bar for others to follow. Privacy protections at federal websites should at least follow the guidance provided through the Federal Information Security Management Act and last year's publication of the Cybersecurity Framework by the National Institute of Standards and Technology. I am interested in hearing from our expert witnesses about privacy protections for users of HealthCare.gov.

During my first hearing as Chairwoman of this Subcommittee, I shared that I experienced a credit card breach because someone had ordered $7,000 in wrongful charges on my card right before Christmas.

Fortunately, the situation was resolved and I wasn't liable for those charges. But what if information stolen like this had been related to health?

You can get a new credit card when your old one is hacked. But once personal health information is compromised, it could be out there forever. That is why health and health insurance information is reportedly worth up to ten times as much as credit card information on the black market.

The risks posed by HealthCare.gov data sharing are underscored by the fact that a hacker accessed the website last July to upload malicious software. Government investigators found no evidence that consumers' personal data were taken, but HHS said the attack appears to have been the first successful intrusion into the website. Many security experts have warned of vulnerability to hacking since HealthCare.gov went live more than a year ago.

And just last week, we learned about what might be the largest data breach against the country's second biggest health insurer, Anthem. In this case, stolen information for 80 million Anthem members included names, birth dates, Social Security numbers and medical IDs.

I posted information about the Anthem situation at my official website to inform my constituents.

Today's hearing is a precursor to one at which we will invite witnesses from the federal government to answer specific questions about the HealthCare.gov contracts with third party companies. I look forward to the insights of both our witnesses today as the Committee continues its due diligence over this issue.

###