

**Congress of the United States**  
**Washington, DC 20515**

January 27, 2015

The Honorable Sylvia Matthews Burwell  
Secretary  
U.S. Department of Health and Human Services  
200 Independence Avenue, SW  
Washington, DC 20201

The Honorable Marilyn Tavenner  
Administrator  
Centers for Medicare and Medicaid Services  
200 Independence Avenue, SW  
Washington, DC 20201

Dear Secretary Burwell and Administrator Tavenner:

A recent report by the *Associated Press*<sup>1</sup> (*AP*) found that numerous third-party vendors have access to consumers' private information via HealthCare.gov. The website contains one of the most substantial records of Americans' personal, sensitive information ever compiled by the U.S. government. This revelation raises many serious questions regarding the security and privacy of the American people's information. This is particularly concerning in light of the September 2014 U.S. Government Accountability Office (GAO) report on the security of HealthCare.gov<sup>2</sup>, which detailed how consumers' sensitive information is at risk. It also stands in stark contrast to the Obama Administration's own blueprint for online consumer privacy protections issued in February 2012<sup>3</sup> and HealthCare.gov's own privacy policy<sup>4</sup>.

According to the *AP*, dozens of third-party vendors are able to collect sensitive information about applicants, including the applicant's age, income, zip code, as well as smoking and pregnancy status. The article also stated that technology experts documented that some of the vendors were collecting "highly specific information." The Administration has repeatedly stated that HealthCare.gov adheres to standards set by the National Institute for Standards and Technology (NIST), yet NIST has cautioned that the type of data being collected and shared through the website can be used to definitively identify someone. HealthCare.gov's own privacy policy states that, "No personally identifiable information is collected." The collection and dissemination of such precise, personal information is in conflict with this assertion.

After the release of the *AP* report, the Administration appears to have scaled back its release of data to third-party vendors. There is still considerable concern over how the previously shared consumer information was used and by whom and how consumer information continues to be shared and with

---

<sup>1</sup> Alsonso-Zaldivar, R. & Gillium, J. (2015, January 20). Government health care website quietly sharing personal data. *The Associated Press*. Retrieved from <http://bigstory.ap.org/article/31490a20926d4ed3b98ff2d0ed8fc81d/new-privacy-concerns-over-governments-health-care-website>

<sup>2</sup> U.S. Government Accountability Office. (2014, September). *HealthCare.gov: Actions needed to address weaknesses in information security and privacy controls*. Retrieved from <http://www.gao.gov/assets/670/665840.pdf>

<sup>3</sup> The White House. (2012, February). Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy. Retrieved from <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>

<sup>4</sup> HealthCare.gov (n/d) *HealthCare.gov privacy policy*. Retrieved from <https://www.healthcare.gov/privacy>

whom, however. Further, the fact that consumers were not aware of this practice is extremely troubling. It appears that the Administration ignored its own policy proposals for an explicit right to privacy for consumers.

In February 2012, the White House released a policy blueprint entitled the “Consumer Privacy Bill of Rights.” The document outlines a series of rights that consumers should expect in regards to online privacy, including:

- The “right to exercise control over what personal data companies collect from them and how they use it.”
- The “right to easily understandable and accessible information about privacy and security practices.”
- The “right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.”
- The “right to reasonable limits on the personal data that companies collect and retain.”

These policy proposals are diametrically opposed to the undisclosed data collection and sharing that took place via the country’s largest government website. There are serious questions as to whether similar data sharing practices are occurring on different government websites, including those that regularly communicate with HealthCare.gov such as those run by the Internal Revenue Service and the Department of Homeland Security.

In addition to privacy concerns, the security issues surrounding HealthCare.gov and consumer data remain. The 2014 GAO report concluded that the extraordinary mismanagement of the development of HealthCare.gov resulted in multiple security vulnerabilities. Cybersecurity experts have continually warned that third-party vendors pose a threat to cybersecurity and privacy. The large number of vendors with access to consumer data via HealthCare.gov is disturbing.

To this end, we request the following information:

1. What types of data have been collected by HealthCare.gov?
  - a. How long was this data stored?
  - b. In what way was the data secured?
2. How many and what third-party vendors was the data shared with?
  - a. How often was the data shared or otherwise available to third-party vendors?
  - b. In what manner was the data securely transmitted?
  - c. In what manner was the data used for each listed vendor?
3. What manner of oversight is the Department of Health and Human Services performing on the third-party vendors for both security and use of the data?
  - a. Who is performing the oversight?
  - b. How often are the vendors being audited?
4. Explain with specificity how HealthCare.gov was operated in a manner consistent with the White House’s “Consumer Privacy Bill of Rights” both before media reports highlighted the vulnerability of personal information and since.

In addition to these questions, please provide an accounting of the explicit privacy and security standards that HealthCare.gov and other government websites that share data with it are required to adhere to and details on whether or not these standards were met or were deemed deficient. Please also

explain what standards the third-party vendors adhere to, who assesses adherence to these standards, and any incidents where these standards were not met or were deemed deficient. We further request an overview of any revisions to the privacy policy that will be made to HealthCare.gov in light of these revelations.

We respectfully ask that your office provide answers to these questions by February 11, 2015. We thank you for your prompt attention to this letter and look forward to your timely response. Should you have any questions, please contact Katie Allen at [Kathryn.Allen@mail.house.gov](mailto:Kathryn.Allen@mail.house.gov) in Representative Black's office.

Sincerely,



Diane Black  
Member of Congress



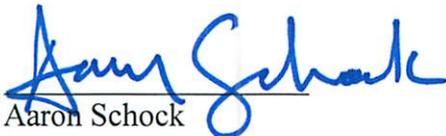
Patrick Meehan  
Member of Congress



Gregg Harper  
Member of Congress



Kristi Noem  
Member of Congress



Aaron Schock  
Member of Congress