Congress of the United States
Washington, DC 20515

MEMORANDUM

January 9, 2014

To: Democratic Members and Staff

Fr: Ranking Members Henry A. Waxman and Elijah E. Cummings

Re: Healthcare.gov Security Issues

On Friday, the House will vote on H.R. 3811, the Health Exchange Security and Transparency Act. This legislation would require that the Department of Health and Human Services (HHS) notify individuals within two days of a known security breach of the Healthcare.gov website. This memo summarizes three key points from our Committees' investigations: (1) there have been no successful security attacks to date on Healthcare.gov; (2) Healthcare.gov does not collect or store detailed personal health information; and (3) HHS already has in place protocols for informing affected citizens as rapidly as possible in the event of a security breach.

I. NO SUCCESSFUL SECURITY ATTACKS ON HEALTHCARE.GOV

On December 11, 2013, members and staff of the Committee on Energy and Commerce received a classified briefing from Dr. Kevin Charest, HHS Chief Information Security Officer, and Ned Holland, HHS Assistant Secretary for Administration. Portions of this briefing were classified to protect information relevant to national security. HHS provided an updated briefing two days ago, on January 7, 2014.

According to Dr. Charest, no person or group has hacked into Healthcare.gov, and no person or group has maliciously accessed any personally identifiable information from users.

HHS officials also have confirmed on multiple occasions during transcribed interviews with the Committee on Oversight and Government Reform that there have been no successful security breaches to date. For example, on December 17, 2013, Teresa Fryer, the Chief Information Security Officer at CMS, stated: "There has been no successful — no successful

breaches, security incidents."[1] Ms. Fryer explained that "[a]ll systems are susceptible to attacks," but there have been "no successful attempts" to date.[2]

On December 19, 2013, Oversight Committee staff conducted a transcribed interview of Darrin Lyles, Information System Security Officer at CMS, who confirmed Ms. Fryer's report in the following exchange:

> Q: Miss Fryer told us, I believe yesterday, that there had been no successful security breaches or incidents.
>
> A: I would agree with that.[3]

In fact, after briefing the Energy and Commerce Committee on Tuesday, Dr. Charest, the HHS Chief Information Security Officer, was interviewed yesterday for more than five hours by Oversight Committee staff, and he agreed that "no malicious actors have successfully attacked the Healthcare.gov system."[4]

Government information technology systems are under constant attack by domestic hackers, foreign entities, and others wishing to harm U.S. national interests, and there have been several reported breaches of defense and other agency systems over the past decade. In the case of the Healthcare.gov website, however, evidence obtained by the Committees shows that there have been no successful security attacks to date. HHS officials are complying with the Federal Information Security Management Act and its implementing regulations, and they are conducting 24-7 system monitoring and ongoing assessments to ensure and strengthen system security.

II. DETAILED PERSONAL HEALTH INFORMATION IS NOT COLLECTED OR STORED ON HEALTHCARE.GOV

While Republican leaders have claimed that the detailed personal medical information of users is at risk on the Healthcare.gov website, this is not the case. This is because the website does not collect detailed information about the health status of consumers. Instead, applicants submit a limited amount of information, such as their names, addresses, income levels, and the number of family members to be covered.

---

[1] House Committee on Oversight and Government Reform, Transcribed Interview of Teresa Fryer, Chief Information Security Officer, Centers for Medicare and Medicaid Services (Dec. 17, 2013).

[2] *Id.*

[3] House Committee on Oversight and Government Reform, Transcribed Interview of Darrin Lyles, Information Systems Security Officer, Centers for Medicare and Medicaid Services (Dec. 19, 2013).

[4] House Committee on Oversight and Government Reform, Transcribed Interview of Dr. Kevin Charest, Chief Information Security Officer, Department of Health and Human Services (Jan. 8, 2014).

Before the Affordable Care Act went into effect, applying for insurance coverage on the individual market was a complicated process that required the disclosure of extensive health information. Insurance companies were allowed to deny coverage to people with preexisting conditions and, in the process, routinely required applicants to fill out long applications that demanded detailed information on dozens of health conditions, from obesity to mental health disorders to high blood pressure, and even a history of domestic abuse.

Under the Affordable Care Act, insurers are now prohibited from discriminating against people with preexisting conditions, so applicants are not required to submit this type of detailed information on the Healthcare.gov website when they apply for coverage.

III. HHS PROCEDURES FOR INFORMING THE PUBLIC IN THE EVENT OF A SECURITY BREACH

Like all federal agencies, HHS already must notify consumers — consistent with the Federal Information Security Management Act, the Privacy Act, and requirements set forth by the Office of Management and Budget (OMB) — of breaches to their personally identifiable information (PII).

OMB Memorandum M-07-16 establishes a minimum framework for notifying individuals of breaches and notes that "agencies may implement more stringent policies and procedures."[5] This protocol requires agencies to provide consumers with "notification without unreasonable delay following the discovery of a breach."[6] Agencies must report all breaches involving PII to US-CERT at the Department of Homeland Security (DHS), and individuals must receive a comprehensive written notification package, including a description of what happened, the dates of the breach and the discovery, how the information was encrypted or protected, next steps for individuals to protect themselves, what the agency is doing to investigate the breach, and who to contact at the agency for more information.[7]

To implement these guidelines, HHS issued its "Personally Identifiable Information (PII) Breach Response Team (BRT) Policy," which states that the agency "shall ensure that notifications are made to the affected individuals."[8] The policy gives HHS up to 60 days to investigate security incidents, such as a missing laptop containing PII. HHS officials say that their practice is to act much more quickly. If HHS confirms that an individual's PII has been breached, HHS notifies the person as rapidly as possible.

---

[5] Office of Management and Budget, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information M-07-16* (May 22, 2007) (online at www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf).

[6] *Id.*

[7] *Id.*

[8] Department of Health and Human Services, *Personally Identifiable Information (PII) Breach Response Team (BRT) Policy HHS-OCIO-2008-0001.003* (Nov. 17, 2008) (online at www.hhs.gov/ocio/policy/20080001.003.html).