DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

SEP 1 0 2013

The Honorable Bennie Thompson
Ranking Member
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

Dear Representative Thompson:

Thank you for your inquiry related to privacy and security protections associated with the Data Services Hub (Hub) and the status of our work to protect people and programs from cyber-attacks in this area. At the Department of Health and Human Services (HHS), we take very seriously our responsibility to safeguard personal information in all of our programs, including in the Affordable Care Act Marketplace. Collectively, the tools, methods, policies, and procedures we have developed provide a safe and sound security framework to safeguard consumer data, allowing eligible Americans to confidently and securely enroll in quality affordable health coverage starting on October 1, 2013. This framework is consistent with the framework that exists for all other HHS programs, such as Medicare, which Americans rely on every day.

HHS's Centers for Medicare & Medicaid Services (CMS) has a strong track record of preventing breaches involving the loss of personally identifiable information from cyber-attacks. This is due in large part to the establishment of an information security program with consistent risk management, security controls assessment, and security authorization processes for all enterprise systems. Our system and security protocols are grounded in statutes, guidelines and industry standards that ensure the security, privacy, and integrity of our systems and the data that flow through them. These protections include a series of statutes and amendments to these laws, such as the Privacy Act of 1974, the Computer Security Act of 1987 and the Federal Information Security Management Act (FISMA) of 2002, as well as various regulations and policies promulgated by HHS, the Office of Management and Budget, the Department of Homeland Security, and the National Institute of Standards and Technology (NIST).

In accordance with these provisions, CMS has developed the Hub, a routing tool that helps Marketplaces provide accurate and timely eligibility determinations. **It is important to point out that the Hub will not retain or store Personally Identifiable Information.** Rather, the Hub is a routing system that CMS is using to verify data against information contained in already existing, secure and trusted federal and state databases. CMS will have security and privacy agreements with all federal agencies and states with which we are validating data. These include the Social Security Administration, the Internal Revenue Service, the Department of Homeland Security, the Department of Veterans Affairs, Medicare, TRICARE, the Peace Corps and the Office of Personnel Management.

The Hub is designed to comply with the comprehensive information security standards developed by NIST in support of FISMA. NIST has emerged as the gold standard

for information security standards and guidelines that all federal agencies follow. Several layers of protection will be in place to help protect against potential damage from attackers and mitigate risks. For example, the Hub will employ a continuous monitoring model that will utilize sensors and active event monitoring to quickly identify and take action against irregular behavior and unauthorized system changes that could indicate potential attacks. Automated methods will ensure that system administrators have access to only the parts of the system that are necessary to perform their jobs. These protocols, combined with continuous monitoring, will alert system security personnel when any system administrator attempts to perform functions or access data for which they are not authorized or are inconsistent with their job functions.

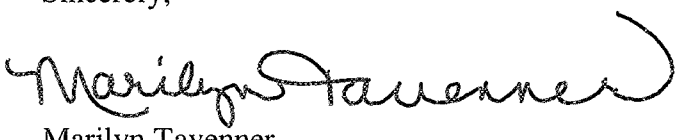
Should security incidents occur, an Incident Response capability built on the model developed by NIST would be activated. The Incident Response function allows for the tracking, investigation, and reporting of incidents so that HHS may quickly identify security incidents and ensure that the relevant law enforcement authorities, such as the HHS Office of Inspector General Cyber Crimes Unit, are notified for purposes of possible criminal investigation.

Before Marketplace systems are allowed to operate and begin serving consumers across the country, they must comply with the rigorous standards that we apply to all federal operational systems and CMS's Chief Information Officer must authorize the systems to begin operation. I am pleased to report that the Hub completed its independent Security Controls Assessment on August 23, 2013 and was authorized to operate on September 6, 2013. The completion of this testing confirms that the Hub comports with the stringent standards discussed above and that HHS has implemented the appropriate procedures and safeguards necessary for the Hub to operate securely on October 1.

The privacy and security of consumer data are a top priority for HHS and our federal, state, and private partners. We understand that our responsibility to safeguard our systems is an ongoing process, and that we must remain vigilant throughout their operations to anticipate and protect against evolving data security threats. Accordingly, we have implemented privacy and security measures for the Marketplace systems that employ measures similar to those in the private sector and we will continually validate through a variety of methods.

In closing, we have produced an extremely strong enterprise information security program by implementing state-of-the-art controls and business processes based on statutory requirements, agency and organizational commitments, best practices, and the experience and knowledge of our subject matter team members. This has resulted in the development, testing and readiness of the Hub to operate on October 1 to serve consumers across the country in a secure and efficient manner. We hope this information is responsive to your inquiry. Thank you for your interest in and leadership on this important issue.

Sincerely,



Marilyn Tavenner