STATEMENT OF

MARILYN TAVENNER

ADMINISTRATOR,
CENTERS FOR MEDICARE & MEDICAID SERVICES

ON

EVALUATING PRIVACY, SECURITY, AND FRAUD CONCERNS WITH OBAMACARE'S INFORMATION SHARING APPARATUS

BEFORE THE

U. S. HOUSE COMMITTEE ON OVERSIGHT & GOVERNMENT REFORM
SUBCOMMITTEE ON ENERGY POLICY, HEALTH CARE, AND ENTITLMENTS

U.S. HOUSE COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

JULY 17, 2013

U. S. House Committee on Oversight and Government Reform,
Subcommittee on Energy Policy, Health Care
U.S. House Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
"Evaluating Privacy, Security, and Fraud Concerns with
Obamacare's Information Sharing Apparatus"
July 17, 2013

Good morning, Chairmen Lankford and Meehan, Ranking Members Speier and Clarke, and members of the Subcommittees. Thank you for the opportunity to discuss the Centers for Medicare & Medicaid Services' (CMS) progress in implementing information technology systems in support of the new Health Insurance Marketplaces. Since the passage of the Affordable Care Act, CMS has been hard at work to design, build, and test secure systems that ensure Americans are able to enroll in affordable health care coverage. Given this important work, I appreciate the interest these Committees and the Congress have shown in our progress in completing and managing these systems. I want to assure you that I am committed to applying all the appropriate laws, regulations, and business agreements to protect the security and privacy of the consumers participating in the Marketplaces. CMS brings to this task experience and success in protecting the security and privacy in programs even larger than the Marketplaces such as Medicare.

Overview of the Marketplace Information Technology (IT) Systems

The Affordable Care Act directs states to establish State-based Marketplaces by January 1, 2014. In states electing not to establish and operate such a Marketplace, the Affordable Care Act requires the Federal government to establish and operate a Marketplace in the state, referred to as a Federally-facilitated Marketplace. The Marketplaces will provide consumers access to health care coverage through private, qualified health plans, and consumers seeking financial assistance may qualify for insurance affordability programs made available through the Marketplace.

The insurance affordability programs include the advance payment of the premium tax credits, cost-sharing reductions, Medicaid, and the Children's Health Insurance Program (CHIP). The

advance payment of the premium tax credit may be applied automatically to the purchase of a qualified health plan through the Marketplace, reducing upfront the premiums paid by consumers. Cost-sharing reductions may also lower the amount a consumer has to pay out-of-pocket for deductibles, coinsurance, and copayments for a qualified health plan purchased through the Marketplace. In order to enroll in an insurance affordability program offered through a Marketplace, individuals must complete an application[1] and meet certain eligibility requirements.[2] Before we get further into this discussion, it is important to note that while the Marketplace application asks for personal information such as date of birth, name, or address, the Marketplace application never asks for personal health information and the Marketplace IT systems will never access or store personal health information beyond what is normally asked for in Medicaid eligibility applications.

Eligibility, Redetermination, and Appeals Marketplace IT Systems

To fulfill the functions specified in the Affordable Care Act, Federally-facilitated and State-based Marketplaces are developing eligibility, redetermination, and appeals systems. These systems are similar to what private issuers, Medicare Advantage issuers, and State Medicaid agencies currently use to determine eligibility, enroll applicants into health coverage, process appeals, and perform customer service, as well as prevent fraud, waste, and abuse.

These systems will:

- Determine a consumer's eligibility to enroll in a qualified health plan through a Marketplace and for insurance affordability programs;
- Redetermine consumer eligibility status during the year;
- Allow individuals to appeal an eligibility determination;
- Enroll consumers in and provide payment transactions for insurance affordability programs; and
- Provide oversight to ensure issuers comply with new Affordable Care Act consumer protections.

[1] The individual application short form is available at this website: http://www.cms.gov/CCIIO/Resources/Forms-Reports-and-Other-Resources/Downloads/marketplace-app-short-form.pdf

[2] Pursuant to 45 C.F.R. 155.305.

Federal Data Services Hub

CMS has developed a tool, known as the Federal data services hub (the Hub), that provides an electronic connection between the eligibility systems of the Marketplaces to already existing, secure Federal and state databases to verify the information a consumer provides in their Marketplace application. Data transmitted through the Hub will help state agencies determine applicants' eligibility to enroll in Medicaid or CHIP, and help the Federally-facilitated and State-based Marketplace eligibility systems determine an applicant's eligibility to seek health insurance coverage through a Marketplace, and their eligibility for advance premium tax credits and cost-sharing reductions.

It is important to understand that the Hub is not a database; it does not retain or store information. It is a routing tool that can validate applicant information from various trusted government databases through secure networks. It allows the Marketplace, Medicaid, and CHIP systems to query the government databases used today in the eligibility processes for many state and Federal programs. The Hub would query only the databases necessary to determine eligibility for specific applicants. The Hub increases efficiency and security by eliminating the need for each Marketplace, Medicaid agency, and CHIP agency to set up separate data connections to each database.

CMS has already completed development and the majority of the testing of the Hub services required to support open enrollment on October 1, 2013. CMS and the Internal Revenue Service (IRS) are currently testing the integration of the Hub with their IT systems, and this testing was 95 percent complete as of the end of June. CMS started testing the Hub with the other Federal partners, including the Social Security Administration (SSA) and the Department of Homeland Security (DHS), earlier this summer, and that testing will be completed by the end of August. CMS is currently testing the Hub with 40 states, and during the remainder of July and August, we will finish testing the Hub with the remaining states and territories.

How These Systems Verify a Marketplace Application

All State-based and Federally-facilitated Marketplaces will determine an applicant's eligibility for enrollment in a Qualified Health Plan through the Marketplace, and if the applicant requests,

to determine eligibility for an insurance affordability program. Consumers will be able to access an application through their Marketplace website, by phone, in person or by mailing a paper form. Regardless of the method a consumer uses to apply for coverage, when consumers submit their Marketplace applications, the following steps occur:

1. Social Security Numbers and U.S. citizenship or immigration status will be verified through secure connections using the Hub with the already existing databases of the SSA and the DHS. The Hub will not store or retain the data transmitted in this process.
2. For consumers seeking financial assistance through an insurance affordability program, IRS, using the Hub, will provide information to verify the income of the consumer. If a consumer does not want to apply for financial assistance, then the consumer will not be asked to provide income information. Again, the Hub will not store or retain the data used in this process.
3. If the consumer appears to be eligible for an insurance affordability program, then the Marketplace eligibility system validates the consumer's application by using the Hub to check if the applicant is enrolled in certain health care programs provided by the Department of Veterans Affairs (VA) or eligible for coverage through other programs provided by the Department of Defense (DOD), Office of Personnel Management (OPM), Peace Corps, Medicare, or state Medicaid agencies. Alternative processes have been established through rulemaking for eligibility factors not verifiable through the Hub.

What Information is Stored?

As clarified above, the Hub is a tool, not a database, and will therefore not store any information, since it only routes requests from Marketplace eligibility systems to already-existing Federal and state databases. The Federally-facilitated and State-based eligibility, redetermination, and appeals systems do store certain eligibility and enrollment records, including Federal appeals records, Federal consumer services records, and issuer financial information in order to fulfill their specific functions. These data will only be used to conduct these functions.[3] Access to data in the Federally-facilitated system will be limited to authorized CMS personnel through

[3] The system of records for the Federally-facilitated Marketplace IT system is more thoroughly described in the System of Records Notice (SORN) available at: http://www.gpo.gov/fdsys/pkg/FR-2013-02-06/html/2013-02666.htm.

password security, encryptions, firewalls, and secured operating systems. Personnel having access to the system have been trained in the Privacy Act and information security requirements. This limited data storage is similar to what private issuers, Medicare, and Medicaid agencies currently use to determine eligibility, enroll applicants into health coverage, process appeals, and perform customer service, as well as prevent fraud, waste, and abuse.

Safeguarding the Marketplace IT Systems

The privacy and security of consumer data is a top priority for CMS and our Federal, state, and private partners. We will use appropriate policies, procedures, standards and implementation specifications to ensure the privacy and security of consumer data in accordance with applicable law.

Implementing Privacy Controls for the Marketplace IT Systems

The Congress acknowledged the importance of protecting personal information through the Privacy Act of 1974, which establishes requirements that govern the collection, use, and disclosure of information about individuals that is maintained by a Federal executive agency in a "system of records." Since then, the Congress has passed amendments to the Privacy Act and additional legislation to assure Americans that information collected, created, used, and disclosed by Federal agencies is appropriately safeguarded. These additional protections include the Computer Matching Act, which amended the Privacy Act, and the e-Government Act of 2002. IT projects undertaken by Federal agencies and their contractors in support of the Affordable Care Act will comply with these and all other applicable Federal laws, so that the American public is assured that their personal information is protected.

Additionally, certain classes of data may be subject to additional restrictions or protection on data use or transmission. For example, information systems containing tax return information must also comply with the taxpayer privacy and safeguards requirements of Section 6103 of the Internal Revenue Code.

In order to establish controls and checkpoints within the Marketplace IT systems, CMS established a series of agreements, business processes, and protocols to ensure privacy controls

have been met. Because the databases connected to the Marketplace eligibility systems by the Hub are secure and closed government databases that already exist and comply with Federal privacy standards, most of the work of implementing privacy controls is conducted through business agreements between CMS and its Federal and state partners to assure data is being handled appropriately by all parties before data is exchanged through the Hub. To fulfill the Computer Matching Act requirements, CMS is establishing Computer Matching Agreements between CMS and each Federal and state partner. These Computer Matching Agreements describe how each Federal and state partner will exchange information, using the Hub, in a way that ensures the privacy, integrity, and verification of data disclosed during this exchange. CMS and our Federal partners have signed additional agreements about the use of data and information exchanges, as applicable. CMS began formalizing these processes with our partners in July 2011, and has refined and updated them as the Marketplace IT work has progressed.

To ensure these agreements are met, CMS conducts Privacy Impact Assessments. Before State-based Marketplaces are able to use the Hub, CMS conducts a Privacy Impact Assessment to ensure that the State-based Marketplace has met all federal privacy requirements. CMS is currently reviewing the State-based Marketplaces' Privacy Impact Assessments. Before the Hub is used to route information from Federal databases to Marketplace eligibility systems, CMS completes Federal Privacy Impact Assessments to ensure this information exchange meets the agreed-upon privacy requirements.

Implementing Security Controls for the Marketplace IT Systems

The Congress established security standards for Federal agencies through the Federal Information Security Management Act of 2002 (FISMA). FISMA requires each Federal agency to develop, document, and implement an agency-wide program to secure the information and information systems that support the agency's operations and assets, including those provided or managed by another agency, contractor, or other source. To implement FISMA, the National Institute of Standards and Technology (NIST) has published a series of documents[4] that provide security guidance to Federal Chief Information Security Officers. These

[4] NIST's Special Publication 800-53: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

publications provide security controls for Federal information systems derived from legislation, Executive Orders, policies, directives, regulations, standards, and business needs to protect organizations, individuals, and the nation from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors (both intentional and unintentional). Using these materials, CMS outlined privacy and security principles that every Marketplace will use to develop privacy and security standards for any entity that collects or has access to Marketplace-related personally identifiable information.[5]

CMS will ensure that the IT used for the Marketplaces comply with applicable Federal laws, NIST controls, and security agreements through a stringent monitoring and evaluation system. CMS has a robust security monitoring system that reviews all security events, tools, requirements, and network device logs to identify, assess, and manage vulnerabilities and threats. For example, CMS publishes a monthly Continuous Monitoring Report to describe emerging concerns from a global and local perspective, along with recommendations or mitigation strategies. In addition, CMS conducts real-time monitoring to ensure that security tools are maintained through updates and patches. If changes must be made to Marketplace IT code, CMS uses a "structured change management process," which identifies, evaluates, tests, and models codes changes and is overseen and approved by a business and technical governance board, as required by NIST standards. When the Federally-facilitated Marketplace systems are operational on October 1, 2013, they will be part of the overall established CMS operational security. CMS also benefits from independent reviews by external entities to verify security policy and readiness.

Conclusion

CMS is committed to creating safe, secure, and resilient Marketplace IT systems and protecting personal privacy and confidentiality in collaboration with our partners while expanding access to health insurance coverage to Americans. Collectively, the tools, methods, policies procedures, and laws I have described provide a robust security framework, which helps to safeguard the Marketplace systems and data. I am confident that through our hard work and the use of industry

[5] Please see the guidance listed under "Minimum Acceptable Risk Standards" for more information: http://www.cms.gov/cciio/Resources/Regulations-and-Guidance/index.html#Affordable Insurance Exchanges

best practices, the Marketplace IT systems will help more Americans securely enroll in and afford the health care coverage that fits their needs. Thank you for your attention to this important issue. I would be happy to answer your questions now, and will be able to provide updates about this important topic as we steadily progress towards the beginning of open enrollment on October 1, 2013.

Marilyn Tavenner

Biography

Marilyn Tavenner is currently the Administrator for the Centers for Medicare & Medicaid Services. Previously, Ms. Tavenner was Principal Deputy Administrator for the Centers for Medicare & Medicaid Services (CMS). As the Principal Deputy Administrator, Ms. Tavenner served as the agency's second-ranking official overseeing policy development and implementation as well as management and operations.

Ms. Tavenner, a life-long public health advocate, manages the $820 billion federal agency, which ensures health care coverage for 100 million Americans, with 10 regional offices and more than 4,000 employees nationwide. CMS administers Medicare, and it provides funds and guidance to all states for their Medicaid and Children's Health Insurance (CHIP) programs. With the passage of the Affordable Care Act in March of 2010, Ms. Tavenner is also responsible for overseeing CMS as it implements the insurance reforms and Affordable Insurance Exchanges included in the health reform law.

Prior to assuming her CMS leadership role, Ms. Tavenner served for four years as the Commonwealth of Virginia's Secretary of Health and Human Resources in the administration of former Governor Tim Kaine. In this top cabinet position, she was charged with overseeing 18,000 employees and a $9 billion annual budget to administer Medicaid, mental health, social services, public health, aging, disabilities agencies, and children's services.

Before entering government service, Ms. Tavenner spent 25 years working for the Hospital Corporation of American (HCA). She began working as a nurse at the Johnson-Willis Hospital in Richmond, Va., in 1981 and steadily rose through the company. By 1993, she began working as the hospital's Chief Executive Officer and, by 2001, had assumed responsibility for 20 hospitals as President of the company's Central Atlantic Division. She finished her service to HCA in 2005 as Group President of Outpatient Services, where she spearheaded the development of a national strategy for freestanding outpatient services, including physician recruitment and real estate development.

Ms. Tavenner holds a bachelor's of science degree in nursing and a master's degree in health administration, both from the Virginia Commonwealth University.

She has worked with many community and professional organizations, serving as a board member of the American Hospital Association, as president of the Virginia Hospital Association, as chairperson of the Chesterfield Business Council, and as a life-long member of the Rotary Club. Her contributions also include providing leadership in such public service organizations as the March of Dimes, the United Way and the Juvenile Diabetes Research Foundation. In addition to numerous business awards, Ms. Tavenner has been recognized for her volunteer activities, including the 2007 recipient of the March of Dimes Citizen of the Year Award.