Ranking Member Yvette D. Clarke (D-NY) Opening Statement

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

"The Threat to Americans' Personal Information: A Look into the Security and Reliability of the Health Exchange Data Hub"

Wednesday, September 11, 2013

When President Obama signed the Affordable Care Act in the East Room of the White House on March 23, 2010, the federal government started planning to operate health care insurance marketplaces, also called exchanges, and assist states that opted to run their own marketplaces.

All of this involves developing a complex computer web-based service that would allow millions of Americans access to affordable health care, in the most efficient and safe way possible.

This is a large undertaking, and involves a complicated inter-agency IT and web-based software effort, commonly known as a 'federal data services hub' based at The Department of Health and Human Services, Center for Medicare and Medicaid Services, or CMS.

What is important about this effort is that we must create, collect, and use or disclose personal information of millions of our citizens in a responsible and confidential way.

The health care marketplaces must establish and implement cyber and personal information protection standards that are consistent with specific principles outlined in our current health care law.

Those principles, which are comparable to the ones upon which the HIPAA, the Health Insurance Portability and Accountability Act provide, and they include:

Providing a right of access to one's Personally Identifying Information - commonly referred to as Pii, a right to have erroneous information corrected, and providing accountability through appropriate monitoring and reporting of information breaches.

Exchanges must also establish and implement reasonable operational, technical, administrative, and physical safeguards to ensure the confidentiality, integrity, and availability of Pii, and to prevent unauthorized or inappropriate access, use, or disclosure of Pii.

In addition, Health Exchanges must monitor, periodically access, and update their security controls, and must develop and use secure electronic interfaces when sharing Pii electronically.

CMS has completed its technical design, and build of Federal Data Services Hub and has established an interagency security framework as well as the protocols for connectivity.

Importantly, in a letter to Ranking Member Thompson this morning, HHS has revealed that as of Friday, September 6, they had taken the necessary steps to obtain security authorization for the Data Hub, and the CMS Chief Information Officer has signed the security authorization. This is an important milestone, and it shows that CMS will be ready to operate the hub securely on October 1st.

This will provide a common, secure connection for Marketplaces to seek information from federal databases necessary to verify eligibly for the millions of Americans can begin to shop for quality, affordable health coverage in just a few weeks.

The Hub has several layers of protection to mitigate information security risk. For example, Marketplace systems will employ a continuous monitoring model that will utilize sensors and active event monitoring to quickly identify and take action.

Let us remember, it's simple…the Data Services Hub will transfer data and be used to verify applicant information data for eligibility. The Data Services Hub is NOT a database, it will not function as a database, and it will not contain health care records.

The Hub will send queries and responses among given marketplaces and data sources to determine eligibility. The Data Services Hub will not determine consumer eligibility, nor will it determine which health plans are available in the marketplaces.

CMS and its vendors have told us, and testified before this Subcommittee and Energy and Commerce Subcommittees, that delivery milestones for the Data Services Hub completion are being met on time, and they expect the Data Services Hub will be ready as planned by October 1st.

I am looking forward to the testimony of the HHS Office of Inspector General to learn more about their important role in the implementation of the Federal Data Hub.

Also, we are going to hear testimony today from the Director of the State Medicaid Directors Association, whose Members have been working on this effort from the ground up.

I am eager to learn about the massive efforts that states, and the federal Centers for Medicare and Medicaid Services, have made to stand-up this complex Data Hub.

This is the kind of information we need to help us deliver health care to citizens who really need it.

Ranking Member Yvette D. Clarke (D-NY) Opening Statement

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

"The Threat to Americans' Personal Information: A Look into the Security and Reliability of the Health Exchange Data Hub"

Wednesday, September 11, 2013

When President Obama signed the Affordable Care Act in the East Room of the White House on March 23, 2010, the federal government started planning to operate health care insurance marketplaces, also called exchanges, and assist states that opted to run their own marketplaces.

All of this involves developing a complex computer web-based service that would allow millions of Americans access to affordable health care, in the most efficient and safe way possible.

This is a large undertaking, and involves a complicated inter-agency IT and web-based software effort, commonly known as a 'federal data services hub' based at The Department of Health and Human Services, Center for Medicare and Medicaid Services, or CMS.

What is important about this effort is that we must create, collect, and use or disclose personal information of millions of our citizens in a responsible and confidential way.

The health care marketplaces must establish and implement cyber and personal information protection standards that are consistent with specific principles outlined in our current health care law.

Those principles, which are comparable to the ones upon which the HIPAA, the Health Insurance Portability and Accountability Act provide, and they include:

Providing a right of access to one's Personally Identifying Information - commonly referred to as Pii, a right to have erroneous information corrected, and providing accountability through appropriate monitoring and reporting of information breaches.

Exchanges must also establish and implement reasonable operational, technical, administrative, and physical safeguards to ensure the confidentiality, integrity, and availability of Pii, and to prevent unauthorized or inappropriate access, use, or disclosure of Pii.

In addition, Health Exchanges must monitor, periodically access, and update their security controls, and must develop and use secure electronic interfaces when sharing Pii electronically.

CMS has completed its technical design, and build of Federal Data Services Hub and has established an interagency security framework as well as the protocols for connectivity.

Importantly, in a letter to Ranking Member Thompson this morning, HHS has revealed that as of Friday, September 6, they had taken the necessary steps to obtain security authorization for the Data Hub, and the CMS Chief Information Officer has signed the security authorization. This is an important milestone, and it shows that CMS will be ready to operate the hub securely on October 1st.

This will provide a common, secure connection for Marketplaces to seek information from federal databases necessary to verify eligibly for the millions of Americans can begin to shop for quality, affordable health coverage in just a few weeks.

The Hub has several layers of protection to mitigate information security risk. For example, Marketplace systems will employ a continuous monitoring model that will utilize sensors and active event monitoring to quickly identify and take action.

Let us remember, it's simple…the Data Services Hub will transfer data and be used to verify applicant information data for eligibility. The Data Services Hub is NOT a database, it will not function as a database, and it will not contain health care records.

The Hub will send queries and responses among given marketplaces and data sources to determine eligibility. The Data Services Hub will not determine consumer eligibility, nor will it determine which health plans are available in the marketplaces.

CMS and its vendors have told us, and testified before this Subcommittee and Energy and Commerce Subcommittees, that delivery milestones for the Data Services Hub completion are being met on time, and they expect the Data Services Hub will be ready as planned by October 1st.

I am looking forward to the testimony of the HHS Office of Inspector General to learn more about their important role in the implementation of the Federal Data Hub.

Also, we are going to hear testimony today from the Director of the State Medicaid Directors Association, whose Members have been working on this effort from the ground up.

I am eager to learn about the massive efforts that states, and the federal Centers for Medicare and Medicaid Services, have made to stand-up this complex Data Hub.

This is the kind of information we need to help us deliver health care to citizens who really need it.