FACT SHEET

FOR IMMEDIATE RELEASE   Contact: CMS Media Relations

September 11, 2013   (202) 690-6145 or Press@cms.hhs.gov

<u>**Security of the Marketplace Data Services Hub**</u>

The Centers for Medicare & Medicaid Services (CMS) has built a tool called the Data Services Hub (the Hub) that will help verify information used to determine eligibility for enrollment in qualified health plans and insurance affordability programs. The Hub will provide one connection to the common federal data sources needed to verify consumer application information for income, citizenship, immigration status, access to minimum essential coverage, etc.

It is a critical priority that all systems are secure and personal information is protected. The Hub was specifically designed to minimize security risk, by developing a system that does not retain or store Personally Identifiable Information.

These efforts provide a security framework to safeguard consumer data, allowing eligible Americans to confidently and securely enroll in quality affordable health coverage starting on October 1, 2013. The following describes some of the steps taken to ensure the security of the Hub.

Hub Design

CMS has designed the Hub, a routing tool that helps Marketplaces provide accurate and timely eligibility determinations. The Hub will 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 connecting to the Hub.   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 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. Risk increases when the number of connections to a data source increase – which is why CMS has designed the Hub to prevent such liabilities. The Hub provides one highly secured connection to trusted federal and state databases instead of requiring each agency to set up what could have amounted to hundreds of independently established connections.

Systems Security

The Hub and its associated systems have several layers of protection in place 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 against irregular behavior and unauthorized system changes that could indicate a potential incident.

If a security incident occurs, an Incident Response capability would be activated, which allows for the tracking, investigation, and reporting of incidents. This allows CMS and the Department of Health and Human Services (HHS) to 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.

The privacy and security of consumer data is a top priority for HHS and CMS. The Hub and its associated systems have been built with state-of-the art business processes based on federal and industry standards. CMS has developed an extremely strong enterprise information security program to protect consumer information in a secure and efficient manner during open enrollment and beyond.

Data Hub Testing

Every federal information technology system must comply with rigorous standards before the system is allowed to operate. The Hub completed its independent Security Controls Assessment on August 23, 2013 and received an authorization to operate on September 6, 2013. The completion of this testing confirms that the Hub complies with federal standards and that HHS and CMS have implemented the appropriate procedures and safeguards necessary for the Hub to operate securely on October 1.

As with all systems, the responsibility to safeguard information is an ongoing process, and HHS and CMS will remain vigilant throughout operations to anticipate and protect against evolving data security concerns. The marketplace monitoring program will continually be reviewed for effectiveness of the systems' security controls, through methods that include independent penetration testing, automated vulnerability scans, system configuration monitoring, and active web application scanning.

Compliance

CMS developed the marketplace systems consistent with federal statutes, guidelines and industry standards that ensure the security, privacy, and integrity of systems and the data that flows through them. All of CMS' marketplace systems of records are subject to the Privacy Act of 1974, the Computer Security Act of 1987, and the Federal Information Security Management Act of 2002. These systems must also comply with various rules and regulations promulgated by HHS, the Office of Management and Budget, the Department of Homeland Security, and the National Institute of Standards and Technology.

# # #