Smart Cards will Reduce Medicare Fraud

Today Medicare fraud is out of control. Estimated to be as much as $60 billion dollars per year, funds stolen out of the Medicare program hurt seniors and abuse tax payers. It is truly a crisis. Solving the Medicare fraud crisis requires a thoughtful, multi-pronged approach that must include identity verification and secure Medicare credential for patients, providers and business associates.

The Problem

- Medicare fraud is estimated by the Department of Justice to be $60B/year.
- Seniors are targeted for identity theft & fraud through Medicare.
- Medical records are becoming electronic and moving online, creating a greater target for hackers.
- The Medicare beneficiary population is increasing; expected to be 79 million by 2030 up from 44 million today. (AARP)

A significant prong that must be part of any Medicare fraud crisis solution is knowing who is authorized and eligible to provide and receive benefits. In many cases Medicare numbers are used without the consent of the provider or the patient. On the current card Medicare prints the beneficiary's social security number on the front and instructs the patient to carry it on their person at all times. The card includes no security features and does nothing to prevent the personal information of seniors from being place at risk. Protecting seniors and eliminating fraud in the Medicare program are paramount. Both can be accomplished by requiring proper identity management and secure card technology.

Recent discussions have focused on upgrading the Medicare card to include the same underling smart card technology used by the Department of Defense, the Federal Government for all agency personnel and the US e-Passport. Verifying identity through a secure smart card will protect information, prevent fraud and legitimize claims within the program. Such a program for Medicare would use the same underlying standards as the other government programs but, with a system tailored to the unique needs of the Medicare community.

Smart Card ID Solution

- Smart cards were designed and invented to eliminate fraud.
- Deployed around the world for financial services, mobile communications, healthcare, e-government, and identity management smart cards are used to authenticate access and verify eligibility.
- Smart cards enable secure ID verification in a way that protects personal privacy.
- Only the card holder is able to verify a transaction using a PIN code or biometric.
- Smart cards are electronic credentials that cannot be copied, altered or hacked and provide the necessary electronic verification securing the transaction with two-factor authentication.
- Requiring the card and the cardholder PIN or associated biometric eliminates fraudulent transactions.
- Around the world banks are transitioning from mag-stripe credit cards to chip based smart cards for security reasons to prevent fraud.

Policy Initiatives

- As part of the transition to Health IT –HHS and ONC are looking at identity verification as necessary for electronic health record authorization both online and offline.
- Standards developed by the Federal government are in place today for citizen credentials through the *Identity Credential and Access Management* (ICAM) under the Federal CIO Council.

- Currently, smart cards are issued to first responders to allow access to emergency sites based on federal standards through the *First Responder Authentication Credential* (FRAC) program.
- Under an Interim Final Rule the *Drug Enforcement Agency* (DEA) is requiring two-factor authentication for e-Prescribing which will require smart card based tokens to verify the prescription as legitimate.
- Recently released the White House *National Strategy for Trusted Identities in Cyberspace* calls smart cards a critical component of identity ecosystem, important to securing online transactions and electronic health records.

Like with healthcare, we must establish a ***culture of prevention*** that denies fraudsters the ability to process transactions if they are not the authorized holder of the Medicare number. Currently, we are practicing a ***culture of detection***, or 'pay and chase' which forces us to try and track down the errors and criminals after their claims are approved and paid. This culture of detection is bankrupting us, literally.

Smart Card Medicare Pilot

While smart cards have been deployed for healthcare services around the world, the U.S. is just now recognizing the benefits. An important step forward in the Medicare fraud crisis would be to establish a smart card pilot program. Such a program would prove the benefits including; cost savings, fraud prevention, privacy protection and information security for the Medicare program. Any pilot program must be competitive and based on standards already established and used by the Federal government.

Smart Card Benefits

- Secure, portable, standards-based technology providing the cornerstone of a healthcare identity management system.
- Protect patient information while enabling the authorized sharing of data across multiple electronic health information platforms.
- Provides high assurance when beneficiaries are accessing personalized information regarding their Medicare benefits and services at mymedicare.gov.
- Deliver significant cost savings by improving data accuracy, reducing medical errors and positively identifying patients and providers.
- Provide a viable solution to the identity, security and privacy challenges the healthcare industry faces.
- Create a pilot to prove government cost savings, fraud prevention, privacy protection and information security.

Statistics

- Every $1 the U.S. government invests in combating Medicare and Medicaid fraud saves $1.55. *(U.S. Department of Health & Human Services, 2009)*
- Medicare spends less than one fifth of a cent of every dollar of its $456 billion annual budget combating fraud, waste and abuse. *(Miami Herald, August 11, 2008)*
- Medicare paid 478,500 claims from deceased physicians totaling up to $92 million from 2000 to 2007. These claims included 16,548 to 18,240 deceased physicians. *(U.S. Senate Permanent Committee on Investigations, 2008)*
- Nearly one of three claims (29 percent) Medicare paid for durable medical equipment was erroneous in FY 2006. *(Inspector General report, Department of Health and Human Services, August 2008)*
- According to a Ponemon Institute Study, 5.8% of American Adults are victims of Medical ID Theft (approx 1.5 million adults) with an average cost per victim of $29,160. *(Ponemon Institute's Study: National Study on Medical Identity Theft - Mar 2010)*

- Of those victims 11% reported receiving a misdiagnosis and 13% reported receiving improper treatment due to inaccurate information in their chart as a result of the theft. *(Ponemon Institute's Study: National Study on Medical Identity Theft - Mar 2010)*
- From 2008 to 2009 the number of Medical ID theft cases doubled. Medical ID theft accounts for 7% of all identity theft. *(Javelin: 2010 Identity Fraud Survey Report - Feb 2010)*

For more information please contact: Kelli Emerick - Executive Director, Secure ID Coalition
kemerick@secureidcoalition.org phone: 202.262.9115