

QUESTIONS AND ANSWERS

ON THE IMPLEMENTATION OF A COMMON ACCESS CARD TO PREVENT FRAUD, WASTE AND ABUSE IN THE MEDICARE PROGRAM

Saving Billions for Medicare and Protecting Identity

What is the scope of fraud and waste in the Medicare payments system today?

Medicare fraud is estimated by the Department of Justice to be a \$60 billion per year problem for American tax payers and the U.S. government. (Other groups estimate Medicare fraud could be double that figure.) In 2010 improper payments within Medicare were estimated to be \$48 billion per year according to the Office of Management and Budget.

How do Medicare fraud and improper payments happen?

Medicare fraud and improper payments can happen in a number of ways:

Provider-Based Fraud and Error:

- **Phantom billing** is where fraudsters or unscrupulous medical providers bill Medicare for unnecessary or unperformed procedures, medical tests, or equipment (or for equipment that is billed as new but is, in fact, used).
- **Durable medical equipment abuse** can happen when medical equipment used in the home, like wheelchairs or oxygen tents, are billed many times over, while in fact nothing has been delivered to an actual patient.
- **Processing errors and mistakes** account, in many cases, for improper payment. These payments either should not have been made or were made in an incorrect amount. Improper payments also include payments sent to the wrong recipient or payments where supporting documentation is not available.

Patient-Based Fraud:

- **Fraudulent patient billing** can occur where a patient provides his or her Medicare number to a provider in exchange for kickbacks. The provider bills Medicare for any reason and the patient is told to admit that he or she indeed received the medical treatment.
- **Passed-off or stolen Medicare cards** are used by others to get medical care.

How can we prevent this fraud from happening in the first place?

The government can adopt the Medicare Common Access Card to prevent fraud, waste and abuse with Medicare and protect the identity and health information of beneficiaries.

How can a common access card for Medicare help solve this problem?

Authenticating Medicare beneficiaries and providers during enrollment and providing them with secure personalized credentials will reduce fraud by:

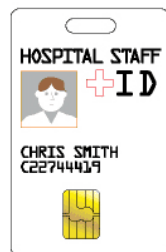
- 1) Verifying beneficiaries are authorized to receive services and pharmaceuticals or equipment being prescribed;
- 2) Verifying providers are authorized to provide those services and bill Medicare;
- 3) Preventing imposters from posing as beneficiaries or providers, thereby thwarting fraudulent transactions; and
- 4) Verifying and coding each transaction to prevent phantom billing, processing errors and DME abuse.

How does authentication work in a secure Medicare card program?

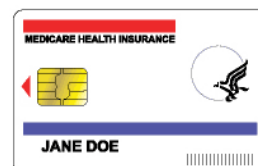
Medicare beneficiaries verify their identity with required documents or certificates on record with the Social Security Administration. Beneficiaries will then receive a secure smart card in the mail which contains their protected identification information on an embedded micro-processor, along with a unique PIN code. The card and PIN together authenticate the beneficiary and authorize the transaction at the doctor's office or pharmacy. This process is known as two-factor authentication.

Medicare Providers verify their identity and eligibility to provide services, during an enrollment process. Provider identity is secured by providing a biometric that will serve as their own unique key to their Medicare billing account. Providers receive a secure smart card which includes an embedded micro-processor that stores basic biographical information, as well as their unique biometric key, thus binding the credential to the individual. The card and the biometric together authenticate the provider (again another type of two-factor authentication).

At the point of service, the transaction is authorized by both the provider and the beneficiary by creating an electronic verification between their two smart cards using the unique keys – in this case, the beneficiary's PIN code and the provider's biometric. This verification is critical as it creates a confirmation by both parties that the service was rendered. The two-factor authentication process (card plus PIN for beneficiaries and card plus biometric for providers) limits the ability of criminals to fraudulently bill Medicare by posing as either a provider or beneficiary.



Provider Card



Beneficiary Card



Insert both cards in reader



**Input beneficiary PIN
& provider biometric**

How does this reduce fraud?

Unauthorized services and product transactions are essentially eliminated as both the secure smart card and the person who owns the key on the card are required to conduct the transaction. This means that phantom billing, fraudulent patient billing and stolen Medicare cards are no longer easy means of bilking Medicare. In addition to imposing strict anti-fraud mechanisms, a Medicare common access card would also reduce processing errors (duplicate or misdirected payments) through digitally signed electronic billing processes.

What are biometrics and how do they work in health care?

Biometrics for Medicare providers are currently being collected under the HHS/CMS Final Rule on Medicare Provider Enrollment Requirements. The pilot program calls for the use of these biometrics in the secure Medicare card system leveraging existing CMS policies to authenticate and certify providers.

The Medicare Common Access Card pilot does not call for use of biometrics for beneficiary authentication.

Biometrics is the science of identifying people based on certain unique physical characteristics. Examples of types of biometric identification include face, fingerprint, hand, retina and iris. The use of biometrics for identification is not a new concept. In fact, unique physical traits have been used to identify individuals for thousands of years. Currently, biometrics are used to identify people in many diverse settings including amusement parks, airports, public schools, hospitals, retail outlets and federal government facilities. Within health care, biometrics are increasingly used for identification due to concerns about patient safety, identity theft, and insurance fraud.

In a secure smart card environment, biometric data is distilled to a mathematical calculation known as a *template*. Because the template is a representation of the biometric and not the actual image, it cannot be reproduced, copied or stolen. The template biometric is securely stored inside a micro-processor embedded in the secure smart card. At the point of verification the card is placed in a card reader. No information on that card can be read until the biometric that was provided at enrollment is presented and read. The smart card and the reader would then perform a one-to-one match (also known as match-on-card) between the template and

the live image. The biometric is confirmation that the person to whom the card belongs is present. Because no one would have the associated biometric except for the rightful individual, the system prevents fraudulent behavior.

Some biometric systems require an online database to which images are matched when they are presented for verification. This process is called a *one-to-many match*. In the case of Medicare this approach is not recommended. The one-to-many match requires constant online access to a central Medicare biometric database. It would require providers to wait for verification of a one-to-many match process which can take significant time. Having a central Medicare biometric database accessible online is also an invitation for hackers and fraudsters to attempt to breach the system.

For a secure, authenticated Medicare system, a one-to-one match using biometric templates is the recommended approach, giving each provider complete control over their card and verification process. Making authentication easy and less time-consuming benefits both beneficiaries and providers.

How does this solution strengthen beneficiary privacy?

A secure Medicare smart card strengthens beneficiary privacy and security in a number of ways.

First, the beneficiary's Social Security number (SSN) is no longer printed on the card and readily available to identity thieves. The identification information will be stored safely on the secure embedded chip.

Second, information on the card can only be read by an authorized Medicare card-reader, and only when the beneficiary consents to input their correct PIN code.

Third, personal information is protected through encryption when transmitted electronically and when stored.

The secure Medicare smart card system similarly protects the privacy and security of the provider's information. Medicare provider numbers and other personal information will no longer be printed on the front of the card; instead, it will be encoded on the card's secure embedded chip. As with beneficiaries, only an authorized Medicare card reader system can access the information on the card, and then only when the provider has consented to present his biometric. These precautions not only protect the legal card holder's privacy, but also ensure the integrity of the system from fraudsters who steal a provider's card in order to make an unauthorized transaction.

Is this technology based on recognized standards? Where else is it used in the U.S. Government?

In the U.S., open standards for secure identity credentials were developed collaboratively by industry standards organizations with the participation of the U.S. government. The standards

were developed to protect both physical and logical (computer networks) government infrastructure against attack. Today every federal agency, including the Department of Defense, utilizes secure smart cards to authenticate and verify users for building access and computer access. While it is hard to measure fraud within government agencies, the DOD confirms a 46% reduction in cyber security attacks on the first day of secured logical access implementations in any given department. The U.S. e-Passport is based on the same underlying secure identification technology and was implemented to prevent unauthorized access into the United States.

Questions about Medicare Recipients and Their Cards

What happens if patients with Alzheimer's or dementia lose their cards - how could that be mitigated against in the system?

This is an issue that exists today with paper Medicare cards containing SSNs in full view. Some cards will get lost, whether it's because of illness or just plain forgetfulness. This is not a technology issue, but a question of policy on how the Center for Medicare and Medicaid Services (CMS) would treat billings that have not been authenticated through a secure smart card system.

In case a beneficiary card is lost, how secure is one's personal information?

If the card is lost, the data on the card is secure and not readable without the individual's PIN code. Further, all information stored in the card cannot be read unless accessed via an authorized, *authenticated* reader. An attempt to hack the chip on the card would destroy the information in the process, because the chips are designed to shut down under brute force attacks. Once the card is reported lost or stolen the system will no longer recognize it and it becomes completely useless. One of the significant benefits that will reduce medical ID theft is that the card will no longer have the beneficiary's social security number printed on it.

In the case of beneficiaries seeking care outside their home region, how will the cards work?

This is an issue that exists today with paper Medicare cards containing SSNs in full view. The secure Medicare smart cards will work in any authenticated provider reader and benefits will be fully available nation-wide under existing Medicare services guidelines.