The Benefits of Strong Authentication for the Centers for Medicare and Medicaid Services

This document was developed by the Smart Card Alliance Health and Human Services Council in response to the GAO report, "Potential Uses of Electronically Readable Cards for Beneficiaries and Providers."

I. Executive Summary

In order to help the Centers for Medicare and Medicaid Services (CMS) improve authentication of beneficiary and provider information at the point of care and secure access to sensitive medical and insurance data, the United States Government Accounting Office (GAO) wrote a report suggesting that electronically readable cards could provide substantially more rigorous authentication, reduce reimbursement errors, and improve medical record-keeping for Medicare. The report, issued in March 2015, details the current issues CMS faces regarding beneficiary and provider identification, security standards, and financial losses due to fraud. This white paper endorses implementing strong authentication for beneficiaries and providers and discusses the benefits.

Verifying the identity of an individual and securing a transaction are vital to preventing fraud, maintaining record accuracy, and reducing risk at the point of care. Standards for implementing solutions that protect a beneficiary's rights and the sensitive information linked to a beneficiary have been slow to emerge. As has been experience in other industries, the only way to implement scalable solutions is through standards[1]. It is important for CMS to understand the profound effects on both the CMS infrastructure and funding of failing to meet the basic identity management challenge—linking the correct individual to the correct data.

Issuing an electronically readable card can provide stronger (more rigorous) authentication. The strength of authentication is measured by the number of factors involved in verifying a person's identity, the reliability of the sources for each factor, and the confidence level that the authentication process is neither compromised nor circumvented. Authentication using smart cards will enable the CMS to use digital identities to automate record matching, increase patient safety, reduce paper file transactions, and allow the correct ICD-10 codes to be linked to the correct insurance information.

Smart card technology has been globally proven to be effective at protecting identity and privacy, and improving administrative and payment processes in healthcare. Smart card technology is well suited for use at CMS. The Smart Card Alliance recommends that the CMS take steps to improve security, mitigate risks associated with identity management, and implement strong authentication.

Additionally, we firmly believe that smart cards provide the secure, interoperable, user-accepted, and easy-to-use solution for the challenges that CMS faces.

[1] Examples include the Personal Identity Verification (PIV) standard for Federal identity, Global System for Mobile (GSM) Communications standard for telecommunications, and Europay MasterCard Visa (EMV) standard for payment.

II. Value Proposition

Strong authentication is used successfully throughout the world in conjunction with credit and debit cards, electronic passports, U.S. government identification cards, and, as detailed in the GAO report, national healthcare cards in Germany, France, Austria, Belgium, and the Czech Republic.

Point-of-care strong authentication requires more than a password or an ID number on a beneficiary card. Strong authentication[2] combines multiple factors (e.g., something you have [such as a cryptographic smart card] and something you know [such as a PIN]), is implemented so that identity information can be proved to be valid, and is based on a process that links the person's identity to the card. Strong authentication can assure a beneficiary's identity at the point of care. Resulting transactions can be signed digitally, ensuring data integrity throughout the system when exchanging medical information and conveying identity and insurance information to providers.

One the many challenges facing the CMS is the increasing financial consequence of fraud. Using the FBI estimate of Medicare fraud as 3–10% of all healthcare billings, the cost of Medicare fraud in 2014 ranges from $18–$60 billion. As important as the actual cost is the enormous gap in the estimates. According to the GAO report, "… there is no reliable measure of the extent of fraud in the Medicare program." Strong authentication can change that and, while it will not eliminate all fraud, it can provide the underlying metrics and patient data necessary to measure the current extent of fraud in the Medicare program and any subsequent reduction.

The most obvious example of how strong authentication can reduce fraud is the establishment of beneficiary identity at the point of care. This authentication ensures that the beneficiary receiving care is the beneficiary who *should* be receiving care, eliminating fraudulent use of benefits. In addition, if the transaction data are signed and encrypted, beneficiary data is protected throughout the transaction.

Other transactions in which strong authentication and associated reporting capabilities reduce fraud include the following:

- Provider billing for services for beneficiaries who were neither seen nor given care
- Provider billing for upcoded services
- Provider billing for unbundled services
- Provider billing of non-covered services as covered services
- Provider paying or receiving kickbacks for beneficiary referrals for specific services, or for purchasing goods or services that may be paid for by Medicare
- Beneficiary soliciting or receiving kickbacks to allow providers to bill for services fraudulently

Strong authentication cannot prevent intentional fraud. However, strong authentication using smart card technology means that transactions can be recorded accurately and signed digitally while also supporting optional claims information and patient arrival reporting. Cleaner transaction records will enable the existing CMS fraud prevention systems to uncover additional suspicious billing patterns. New levels of analytics can be implemented if the foundation data is accurate, as would be the case when strong authentication and smart card technology are used.

---

[2] Additional information on strong authentication can be found in the Smart Card Alliance white paper, "Strong Authentication Using Smart Card Technology for Logical Access," available at http://www.smartcardalliance.org/resources/pdf/Strong_Auth_WP_FINAL_112112.pdf.

III. Discussion of CMS Statements Regarding Digital Identity, Strong Authentication, and Smart Cards

While the Smart Card Alliance views strong authentication provided by electronically readable cards as the cure for many of Medicare's ailments, the conclusions of the GAO report are that "electronically readable cards would have a limited effect on program integrity, but could aid administrative processes." This position is based on a view of electronically readable cards that does not consider the post-processing opportunities offered by a strongly authenticated transaction.

GAO sees the electronically readable card as a front-end component for beneficiary authentication. We see the electronically readable card as an integral part of the infrastructure and transaction chain. If the electronically readable card is only considered for front-end beneficiary authentication, then indeed the effects on Medicare fraud reduction and the overall impact on Medicare program costs will not be significant. However, if the issue is system-wide data integrity, then the impact on fraud will be substantial.

The Smart Card Alliance recognizes that the current CMS system does not properly provide the necessary foundation for system-wide data integrity. However, healthcare providers are currently deploying the infrastructure required to accept contact or contactless smart cards for payment. These payment terminals can be enabled to support secure transactions for healthcare. The additional transaction-processing component required by the CMS should be an extension of the existing platform. As discussed in the GAO report, the CMS should support transactions that include fields for provider location and claim number. In addition, the transactions should be able to include a placeholder reference ID. Because appropriate medical transaction codes are often not known until weeks after a patient visit, the placeholder ID acts as a temporary link until the proper transaction or billing number has been defined. In this way, multiple claims can be modified and included in one transactional event (or episode). The cost associated with such an upgrade is certain to be less than the annual savings achieved through fraud reduction.

The catchall policy statement from the GAO report is the disclaimer that "Using electronically readable cards to authenticate beneficiary and provider presence at the point of care could potentially curtail certain types of Medicare fraud, but would have limited effect since CMS has stated that it would continue to pay claims regardless of whether a card was used." While it's recognized that there may not be 100 percent card adoption and acceptance, it should also be recognized that any improvement of card adoption could translate into a reduction of certain types of Medicare fraud. The Smart Card Alliance agrees that today's fraud is not measureable; however, the assumption is that some percentage of beneficiaries present a card today and would use a card that supports strong authentication in the future. With a card supporting strong authentication, results are measurable and can be improved year over year through incentives, analytics, and law enforcement when fraudulent activity occurs. Incremental program improvements of even a percentage point annually represent $500 million in taxpayer savings. These savings can be allocated to other mission-critical efforts.

The strategy of using a strongly authenticated card has been proven to reduce fraud within the financial markets around the world. The same strategy will work for CMS. The first step is to recognize that different levels of fraud are associated with "card present" and "card not present" transactions. The next step is to add strong authentication for "card present" transactions through the use of smart cards, thereby reducing the level of fraud associated with "card present" transactions.

IV. Other Topics Not Considered in the GAO Report

The GAO report provides the case for the CMS to implement electronically readable cards for beneficiaries and providers. The major benefit, as discussed above, is strong authentication for patient identity verification and data security. Additional benefits not considered in the GAO report include fraud reduction due to strong authentication of providers and a more efficient way to manage claims processing. Both benefits require infrastructure upgrade investments that include both an upfront cost and maintenance fees. The upgrades can be obtained affordably by leveraging the current federal investment in the Personal Identity Verification (PIV) card.

The PIV card is a smart card issued to all Federal employees and contractors that serves as an identity credential and is interoperable across government agencies. PIV cards support both physical and logical access controls. PIV and PIV-interoperable (PIV-I) cards authenticate cardholders to the highest assurance level defined by the U.S. government, Level 4.

The CMS recognizes the PIV card as a legitimate credential, and the CMS and Medicare Administrative Contractors (MAC) have already started to invest in system upgrades to support the card. As stipulated in the *Risk Management Handbook*, *Volume III* of the *CMS Authentication Standards*, entities that fall under the National Institute of Standards and Technology's definition of "non-organizational users" are governed by the Identification and Authentication family of security controls under the CMS Minimum Security Requirements manual, specifically IA-8. Version 2.0 of the CMSR manual now requires the acceptance of PIV credentials from other Federal Agencies.

While they are not yet formally required, strong authentication solutions such as PIV and PIV-I cards represent a robust answer for multifactor authentication. PIV-I cards can enable strong authentication for an insurance providers' interaction with Federal agencies and databases. PIV-I cards leverage the infrastructure created for the Federal PIV card for the benefit of non-Federal entities doing business with the government. Using the Federal Bridge, PIV-I systems can establish the trustworthiness of the PIV-I card and the basic identity of the cardholder. By eliminating opportunities for non-approved entities to access sensitive data, use of PIV-I cards can help the CMS substantially reduce fraud. It is of benefit to the CMS to support and enforce these standards.

In short, this technology holds significant promise for the CMS. Moreover, early adoption creates a competitive advantage for public and private health insurance providers. This includes CMS.

V. Conclusion

It has increasingly been recognized by the U.S. government and within the healthcare industry, that identity management is a critical component of a secure infrastructure. The GAO has issued a report that outlines the benefits of a standards-based electronically readable card for Medicare beneficiaries and providers. Implementing a smart card program will increase the security of records, improve patient matching, decrease healthcare fraud, and reduce medical errors.

The healthcare industry is changing. For example, provider organizations are now required to comply with meaningful use and EHRs. New initiatives will face challenges. However, implementing a strong authentication solution will increase the security of the existing CMS system. In addition, healthcare providers are putting in place smart card-enabled payment terminals that could also accept electronically readable Medicare cards and emerging mobile applications for healthcare.

Through electronically readable cards, the CMS can maximize the security of individual interactions with sensitive CMS data. The move forward can be achieved with incremental steps that will not require a

complete overhaul of the existing CMS infrastructure. Strong authentication creates a foundation that prevents fraud. Tools can be added to the infrastructure to provide further transactional analysis, reporting, and identity assurance. As the GAO report notes, electronically readable cards should be considered a future solution for CMS; recognition and acceptance of this technology are the simplest and most affordable first steps to increasing security and reducing fraud.

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use, and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations, and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information, please visit http://www.smartcardalliance.org.

About the Smart Card Alliance Health and Human Services Council

The Smart Card Alliance Health and Human Services Council brings together human services organizations, payers, healthcare providers, and technologists to promote the adoption of smart cards in U.S. health and human services organizations and within the national health IT infrastructure. The Health & Human Services Council provides a forum where all stakeholders can collaborate to educate the market on the how smart cards can be used and to work on issues inhibiting the industry.