United States Government Accountability Office

Report to Congressional Requesters

March 2015

MEDICARE

Potential Uses of Electronically Readable Cards for Beneficiaries and Providers

Accessible Version

GAO-15-319

March 2015

MEDICARE

Potential Uses of Electronically Readable Cards for Beneficiaries and Providers

GAO Highlights

Highlights of GAO-15-319, a report to congressional requesters

Why GAO Did This Study

Proposals have been put forward to replace the current paper Medicare cards, which display beneficiaries' Social Security numbers, with electronically readable cards, and to issue electronically readable cards to providers as well. Electronically readable cards include cards with magnetic stripes and bar codes and "smart" cards that can process data. Proponents of such cards suggest that their use would bring a number of benefits to the program and Medicare providers, including reducing fraud through the authentication of beneficiary and provider identity at the point of care, furthering electronic health information exchange, and improving provider record keeping and reimbursement processes.

GAO was asked to review the ways in which electronically readable cards could be used for Medicare. This report (1) evaluates the different functions and features of electronically readable cards, (2) examines the potential benefits and limitations associated with the use of electronically readable cards in Medicare, (3) examines the steps CMS and Medicare providers would need to take to implement and use electronically readable cards, and (4) describes the lessons learned from the implementation and use of electronically readable cards in other countries. To do this, GAO reviewed documents, interviewed stakeholders, and conducted visits to two countries with electronically readable card systems.

View GAO-15-319. For more information, contact Kathleen M. King at (202) 512-7114 or kingk@gao.gov.

What GAO Found

The Centers for Medicare & Medicaid Services (CMS)—the agency that administers Medicare—could use electronically readable cards in Medicare for a number of different purposes. Three key uses include authenticating beneficiary and provider presence at the point of care, electronically exchanging beneficiary medical information, and electronically conveying beneficiary identity and insurance information to providers. The type of electronically readable card that would be most appropriate depends on how the cards would be used. Smart cards could provide substantially more rigorous authentication than cards with magnetic stripes or bar codes, and provide greater security and storage capacity for exchanging medical information. All electronically readable cards could be used to convey beneficiary identity and insurance information since they all have adequate storage capacity to contain such information.

Using electronically readable cards to authenticate beneficiary and provider presence at the point of care could curtail certain types of Medicare fraud, but would have limited effect since CMS officials stated that Medicare would continue to pay claims regardless of whether a card was used due to legitimate reasons why a card may not be present. CMS officials and stakeholders told us that claims should still be paid even when cards are not used because they would not want to limit beneficiaries' access to care. Using electronically readable cards to exchange medical information is not part of current federal efforts to facilitate health information exchange and, if used to supplement current efforts, it would likely involve challenges with interoperability and ensuring consistency with provider records. Using electronically readable cards to convey identity and insurance information to auto-populate and retrieve information from provider information technology (IT) systems could reduce reimbursement errors and improve medical record keeping.

To use electronically readable cards to authenticate beneficiaries and providers, CMS would need to update its claims processing systems to verify that the cards were swiped at the point of care. CMS would also need to update its current card management processes, including issuing provider cards and developing standards and procedures for card use. Conversely, using the cards to convey beneficiary identity and insurance information might not require updates to CMS's IT systems or card management practices. For all potential uses, Medicare providers could incur costs and face challenges updating their IT systems to use the cards.

The experiences of France and Germany demonstrate that an electronically readable card system can be implemented on a national scale, though implementation took years in both countries. It is unclear if the cost savings reported by both countries would be achievable for Medicare since the savings resulted from using the cards to implement electronic billing, which Medicare already uses. Both countries have processes in place to manage competing stakeholder needs and oversee the technical infrastructure needed for the cards.

The Department of Health and Human Services provided technical comments on a draft of this report, which GAO incorporated as appropriate.

Contents

Tables

Figures

Abbreviations

CMS	Centers for Medicare & Medicaid Services
EHR	electronic health record
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
IT	information technology
NIST	National Institute of Standards and Technology
NPI	National Provider Identifier
ONC	Office of the National Coordinator for Health Information Technology
PIN	personal identification number
PKI	public key infrastructure
SSN	Social Security number
VA	Department of Veterans Affairs
WEDI	Workgroup for Electronic Data Interchange

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

March 25, 2015

Congressional Requesters

To demonstrate Medicare coverage, all Medicare beneficiaries are issued paper Medicare cards that include their name, Medicare number, and eligibility status.[1] Medicare beneficiaries present the cards to providers at the point of care to show proof of eligibility for coverage. Providers use the information on the cards to verify eligibility and to submit claims to receive payment for services provided.[2] The Centers for Medicare & Medicaid Services (CMS)—the agency within the Department of Health and Human Services (HHS) that administers the Medicare program—and its contractors use the information on the cards when confirming beneficiary eligibility, processing claims submitted by providers, and conducting program integrity activities.

The Medicare card displays beneficiaries' Social Security numbers (SSN) as the main component of beneficiaries' Medicare numbers and there have been calls by policymakers to update the card to remove the SSN. Displaying beneficiaries' SSNs introduces risks to the security of beneficiaries' personal information, as the number may, among other things, be obtained and used by thieves to steal beneficiaries' identities. In 2013, we recommended that CMS take steps to develop an information technology solution to remove SSNs from Medicare cards.[3]

[1]Medicare is the federal health insurance program that serves the nation's elderly, certain disabled individuals, and individuals with end-stage renal disease.

[2]We use the term provider to refer to any organization, institution, or individual that provides health care services to Medicare beneficiaries. These include hospitals, physicians, hospices, ambulatory surgical centers, outpatient clinics, and suppliers of durable medical equipment, among others.

[3]See GAO, *Medicare Information Technology: Centers for Medicare and Medicaid Services Needs to Pursue a Solution for Removing Social Security Numbers from Cards*, GAO-13-761 (Washington, D.C.: Sept. 10, 2013). In addition, we previously examined options to remove SSNs from Medicare beneficiary cards, including truncating the SSNs that are displayed on the cards and replacing the SSNs with a new identifier. See GAO, *Medicare: CMS Needs an Approach and a Reliable Cost Estimate for Removing Social Security Numbers from Medicare Cards*, GAO-12-831 (Washington, D.C.: Aug. 1, 2012).

Amid the calls to update the Medicare card to remove beneficiaries' SSNs, proposals have been put forward to increase the functionality of the cards by replacing paper Medicare cards with electronically readable cards, and to issue electronically readable cards to providers as well.[4] Electronically readable cards include, among others, cards that store information on magnetic stripes and bar codes and "smart" cards that use microprocessor chips to store and process data. Proponents of electronically readable cards suggest that using the cards in Medicare would bring a number of benefits to CMS and providers, including reducing Medicare fraud through the authentication of beneficiary and provider identity at the point of care, furthering electronic health information exchange, and improving provider record keeping and reimbursement processes. Authentication is the process of validating or confirming the identity of an individual for a specific transaction—in this case, processing Medicare claims.

You asked us to review the ways in which electronically readable cards could be used in Medicare. In this report we (1) evaluate the different functions and features of electronically readable cards, (2) examine the potential benefits and limitations associated with the use of electronically readable cards in Medicare, (3) examine the steps CMS and Medicare providers would need to take to implement and use electronically readable cards, and (4) describe the lessons learned from the implementation and use of electronically readable cards in other countries.

To evaluate the different functions and features of electronically readable cards, we analyzed the technical capabilities of different types of electronically readable cards. Although there are a variety of card technologies, we focused our review on three commonly used types of electronically readable cards: smart cards, cards with magnetic stripes,

[4]Legislation was introduced in both the 112th and 113th Congresses to require CMS to establish a pilot program to issue smart cards—a type of electronically readable card—to both beneficiaries and providers and to evaluate the potential use of such cards for the Medicare program. See S. 2586, 113th Cong., § 2 (2014); H.R.3024, 113th Cong., § 2 (2013); H.R. 3399, 112th Cong., § 203 (2011); S. 1251, 112th Cong., § 203 (2011) (none of the bills were reported out of the relevant committees of jurisdiction). In addition, a health care management organization, the Medical Group Management Association, has supported the industrywide adoption of electronically readable beneficiary health care cards. See Medical Group Management Association, "Project SwipeIt," accessed Jan. 8, 2015, http://www.mgma.com/universal-content/swipeit/introduction.

and cards with bar codes.[5] We analyzed the capabilities of the cards in terms of three key proposed uses for the cards in Medicare that we identified: (1) authenticating beneficiary and provider presence at the point of care; (2) electronically exchanging beneficiary medical information; and (3) electronically conveying beneficiary identity and insurance information to providers. In conducting our analysis, we reviewed industry, academic, and federal agency documents, including National Institute of Standards and Technology (NIST) documents, on card technologies. We also reviewed NIST standards and guidance regarding electronic identity authentication practices and interviewed officials from NIST and the General Services Administration, the agency responsible for guiding federal agency implementation and use of smart cards for federal employees and contractors.

To examine the potential benefits and limitations associated with the use of electronically readable cards in Medicare and the steps CMS and Medicare providers would need to take to implement and use electronically readable cards,[6] we reviewed industry reports on the potential benefits associated with electronically readable cards and interviewed industry officials. We also interviewed officials from federal agencies and stakeholder organizations with knowledge and expertise related to the potential uses of electronically readable cards, including CMS, Office of the National Coordinator for Health Information Technology (ONC), Department of Veterans Affairs (VA), an organization representing Medicare beneficiaries, health care provider organizations, health care information technology (IT) organizations, electronic health care transaction standards organizations, health care billing and

[5]Our analysis of smart cards focused on smart cards with microprocessor chips that are capable of processing data because federal agencies currently use them for authentication. There are "memory-only" smart cards with memory chips that can store data, but do not contain microprocessor chips to process data. Cards with magnetic stripes, such as credit cards, store information on the stripe, which can be read by swiping the card through a card reader. Cards with bar codes contain an electronically readable representation of data—printed and variously patterned bars and spaces—that can be scanned and read.

[6]Our examination of the steps CMS and Medicare providers would need to take to implement and use electronically readable cards did not include steps that would need to be taken to remove beneficiary SSNs from the Medicare card, which we previously reported on in GAO-13-761 and GAO-12-831. The steps that would need to be taken to remove beneficiary SSNs are card technology neutral—that is, the same steps would need to be taken whether CMS issued an updated paper card or any type of electronically readable card.

management organizations, CMS contractors that investigate potential Medicare fraud, anti-health-care fraud organizations, health care insurers, an organization representing health care insurers, state Medicaid programs that have used electronically readable cards, health care providers that have issued electronically readable cards to patients, and health care IT vendors. (For a full list of organizations interviewed, see app. I.) We also reviewed applicable U.S. health care IT and management studies and white papers. To examine the potential effects of electronically readable cards on reimbursement processes, we also analyzed data from CMS on the number of claims that were rejected from January 1, 2014, through September 29, 2014.[7] We discussed these data with agency officials, reviewed them for reasonableness and consistency, and determined that they were sufficiently reliable for our purposes.

To describe the lessons learned from the implementation and use of electronically readable cards in other countries, we conducted site visits to France and Germany to interview officials from relevant organizations. We chose these countries based on long-standing use of electronically readable cards for health care, a population relative to the number of Medicare beneficiaries in the United States; in the case of France, its use of provider cards; and, in the case of Germany, its use of third-party reimbursement of providers for health care services. During our site visit, we spoke with key stakeholders, including organizations representing health care providers and insurers, entities responsible for implementing the cards, and each country's respective health Ministry and federal auditing body.

During our work, we heard about non-card-based technologies that could also potentially serve some of the same uses as electronically readable cards, such as cell phones and other forms of identity tokens. However, those technologies were outside the scope of this review.

We conducted this performance audit from February 2014 to March 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our

[7]We obtained data on rejected claims, which are claims that do not meet basic formatting or data requirements and are returned to providers for resubmission. The data do not include denied claims, which are claims that CMS adjudicates and determines should not be paid.

findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Medicare covered approximately 54 million beneficiaries in fiscal year 2014 at an estimated cost of $603 billion. The program consists of four parts, Parts A through D. In general, Part A covers hospital and other inpatient stays, and Part B covers hospital outpatient and physician services, durable medical equipment, and other services. Together, Parts A and B are known as traditional Medicare or Medicare fee-for-service. Part C is Medicare Advantage, under which beneficiaries receive their Medicare health benefits through private health plans, and Part D is the Medicare outpatient prescription drug benefit, which is administered through private drug plans. Medicare beneficiaries who enroll in Part C or Part D plans receive separate cards from those plans, in addition to their traditional Medicare card. Generally, an individual's eligibility to participate in Medicare is initially determined by the Social Security Administration, based on factors such as age, work history, contributions made to the programs through payroll deductions, and disability. Once the Social Security Administration determines that an individual is eligible, it provides information about the individual to CMS, which prints and issues a paper Medicare card to the beneficiary.[8] Providers must apply to enroll in Medicare to become eligible to bill for services or supplies provided to Medicare beneficiaries. CMS has enrollment standards and screening procedures in place that are designed to ensure that only qualified providers can enroll in the program and to prevent enrollment by entities that might attempt to defraud Medicare.[9] Under Medicare fee-for-service, providers bill Medicare by submitting claims for reimbursement for the services and supplies they provide to beneficiaries. Providers are not issued identification cards, but instead use an assigned unique provider

[8]The Railroad Retirement Board determines eligibility for Medicare for retired railroad workers and produces cards for its beneficiaries.

[9]See GAO, *Medicare Program Integrity: CMS Continues Efforts to Strengthen the Screening of Providers and Suppliers*, GAO-12-351 (Washington, D.C.: Apr. 10, 2012). In addition, to remain eligible for payment, providers and suppliers must continue to meet CMS's Medicare enrollment requirements and periodically revalidate their enrollment information.

identification number—their National Provider Identifier (NPI) number—on each claim.[10]

Key Proposed Uses for Electronically Readable Cards

Electronically readable cards could be implemented for a number of different purposes in Medicare. We identified three key proposed uses:

- **Authenticating beneficiary and provider presence at the point of care**. Beneficiary and provider cards could be used for authentication to potentially help limit certain types of Medicare fraud, as CMS could use records of the cards being swiped to verify that they were present at the point of care. Using electronically readable cards for authentication would not necessarily involve both beneficiaries and providers, as cards could be used solely to authenticate beneficiaries, or solely to authenticate providers.
- **Electronically exchanging beneficiary medical information**. Beneficiary cards could be used to store and exchange medical information, such as electronic health records, beneficiary medical conditions, and emergency care information, such as allergies. Provider cards could also be used as a means to authenticate providers accessing electronic health record (EHR) systems that store and electronically exchange beneficiary health information.[11]
- **Electronically conveying beneficiary identity and insurance information to providers**. Beneficiary cards could be used to auto-populate beneficiary information into provider IT systems and to automatically retrieve existing beneficiary records from provider IT systems. For example, an electronically readable Medicare beneficiary card could contain the identity and insurance information printed on the current paper Medicare cards—beneficiary name, Medicare number, gender, Medicare benefits, and effective date of Medicare coverage. The primary purpose of this potential use would be to improve provider record keeping by allowing providers the option to capture beneficiary information electronically.

[10]NPI numbers are an industrywide standard used to identify providers. Although the numbers are issued by CMS, all providers—not just Medicare and Medicaid providers—are required to use them for certain administrative and financial transactions.

[11]EHR systems are systems that can be used to electronically collect, store, retrieve, and transfer clinical information related to patients' care, among other things.

The use of electronically readable cards for health care has been limited thus far in the United States.[12] According to stakeholders, the limited use is due, in part, to reluctance among the insurance industry and health care providers to invest in a technology that would depend on a significant investment from both parties to implement. However, some health insurers, including a large insurer, have issued electronically readable cards to their beneficiaries, and some integrated health systems have issued cards to patients to help manage patient clinical and administrative information.[13] In other countries, electronically readable cards have been used as health insurance cards for decades. For example, France and Germany have used smart cards in their health care systems since the 1990s. Appendix II includes additional details about France's and Germany's use of smart cards.

Medicare Program Integrity

Although there is no reliable measure of the extent of fraud in the Medicare program, for over two decades we have documented ways in which fraud contributes to Medicare's fiscal problems.[14] Preventing Medicare fraud and ensuring that payments for services and supplies are accurate can be complicated, especially since fraud can be difficult to detect because those involved are generally engaged in intentional deception. Common health care fraud schemes in Medicare include the following:

- **Billing for services not rendered**. This can include providers billing for services and supplies for beneficiaries who were never seen or rendered care, and billing for services not rendered to beneficiaries who are provided care (such as adding a service that was not provided to a claim for otherwise legitimately provided services). In some types of fraud schemes, individuals may steal a provider's identity and submit claims for services never rendered and divert the reimbursements without the provider's knowledge.

[12]Council for Affordable Quality Healthcare's Committee on Operating Rules for Information Exchange, "Standard Health ID Card Business Case" (Aug. 5, 2009).

[13]Integrated health systems are systems of care in which providers, such as hospitals and physicians, organize to coordinate and share in aspects of care delivery.

[14]For more than 20 years, we have designated Medicare as a high-risk program, in part because its complexity makes it particularly vulnerable to fraud. See GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

- **Fraudulent or abusive billing practices**. This can include providers billing Medicare more than once for the same service; inappropriately billing Medicare and another payer for the same service; upcoding of services; unbundling of services; billing for noncovered services as covered services; billing for medically unnecessary services; and billing for services that were performed by an unqualified individual, or misrepresenting the credentials of the person who provided the services.[15]
- **Kickbacks**. This can include providers, provider associates, or beneficiaries knowingly and willfully offering, paying, soliciting, or receiving anything of value to induce or reward referrals or payments for services or goods under Medicare.[16]

Among other processes, to detect potential fraud, CMS employs IT systems—including its Fraud Prevention System—that analyze claims submitted over a period of time to detect patterns of suspicious billing.[17] CMS and its contractors investigate providers and beneficiaries with suspicious billing and utilization patterns and, in suspected cases of fraud, can take administrative actions, such as suspending payments or revoking a provider's billing privileges, or refer the investigation to the HHS Office of Inspector General for further examination and possible criminal or civil prosecution.

Identity Authentication

As we have previously reported, there are three potential factors that can be used to authenticate an individual's identity: (1) "something they possess," such as a card, (2) "something they know," such as a password

[15]Upcoding is the submission of claims that seek reimbursement for more specialized services, or services involving more time or complexity, than actually provided. Unbundling is billing for bundled services separately to obtain greater reimbursements.

[16]Medicare fraud schemes may involve more than one form of fraud. For example, a provider billing for nonmedically necessary services may also pay kickbacks to another provider to refer beneficiaries for services.

We have ongoing work to describe the types of health care fraud schemes among cases that were handled by federal agencies.

[17]Although the Fraud Prevention System screens claims prior to payment, the system is primarily used to identify and prioritize postpayment investigations of providers at high risk for fraudulent billing. See GAO, *Medicare Fraud Prevention: CMS Has Implemented a Predictive Analytics System, but Needs to Define Measures to Determine Its Effectiveness*, GAO-13-104 (Washington, D.C.: Oct. 15, 2012).

or personal identification number (PIN), and (3) "something they are," such as biometric information, for example, a fingerprint, or a picture ID.[18] Generally, the more factors that are used to authenticate an individual's identity, the higher the level of identity assurance. For example, a card used in conjunction with a PIN provides a higher level of identity authentication than just a card, since the PIN makes it more difficult for individuals who are not the cardholder to use a lost or stolen card.

NIST has issued standards for federal agencies for using electronically readable cards to achieve a high level of authentication, and those standards require robust enrollment and card issuance processes to ensure that the cards are issued to the correct individuals. These processes include procedures to verify an individual's identity prior to card issuance to ensure eligibility and to ensure that the cards are issued to the correct individual. For example, verifying an individual's address is an important practice for issuing cards by mail. If a significant number of cards are issued to ineligible or incorrect individuals, it undermines the utility of the cards for identity authentication.

Practices that provide higher levels of identity authentication generally are more expensive and difficult to implement and maintain and may cause greater inconvenience to users than practices that provide lower levels of assurance. The level of identity authentication that is appropriate for a given application or transaction depends on the risks associated with the application or transaction. The greater the determined risk, the greater the need for higher-level identity authentication practices. The Office of Management and Budget and NIST have issued guidance defining four levels of identity assurance ranging from level 1—"little or no confidence in the asserted identity's validity"—to level four—"very high confidence in the asserted identity's validity"—and directed agencies to use risk-based methods to decide which level of authentication is appropriate for any given application or transaction. Additionally, authentication practices should take into account issues related to cost and user acceptability.

[18]We have previously reported on authentication practices and the use of smart cards in the federal government for physical and logical access to facilities and computer systems. See GAO, *Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards*, GAO-11-751 (Washington, D.C.: Sept. 20, 2011).

CMS currently relies on providers to authenticate the identities of Medicare beneficiaries to whom they are providing care, but the agency does not have a way to verify whether beneficiaries and providers were actually present at the point of care when processing claims. At this point, CMS has not made a determination that a higher level of beneficiary and provider authentication is needed.

Smart Cards Can Provide More Rigorous Authentication, but All Cards Could Electronically Convey Beneficiary Identity and Insurance Information

The type of electronically readable card most appropriate for Medicare would depend on how the cards would be used. Three common types of electronically readable cards that could be used to replace the current printed Medicare card are smart cards, magnetic stripe cards, and bar code cards. The key distinguishing feature of smart cards is that they contain a microprocessor chip that can both store and process data, much like a very basic computer. Based on our analysis of the capability of the three types of cards, we found that while all of the cards could be used for authentication, storing and exchanging medical information, and conveying beneficiary information, the ability of smart cards to process data enables them to provide higher levels of authentication and better secure information than cards with magnetic stripes and bar codes.

Our analysis found that smart cards could provide substantially more rigorous authentication of the identities of Medicare beneficiaries and providers than magnetic stripe or bar code cards (see fig. 1). Although all three types of electronically readable cards could be used for authentication, smart cards provide a higher level of assurance in their authenticity because they are difficult to counterfeit or copy. Magnetic stripe and bar code cards, on the other hand, are easily counterfeited or copied.[19] For example, officials in France told us that they chose to use smart cards as their health insurance cards, in part, because they were less susceptible to counterfeiting, and reported that they have not encountered any problems with counterfeit cards. Additionally, smart cards can be implemented with a public key infrastructure (PKI)—a system that uses encryption and decryption techniques to secure

[19]The statement that smart cards are more difficult to counterfeit or copy refers to the difficulty of counterfeiting or copying the electronically readable features or information on the cards. Physical security features, such as holograms or watermarks, can be used on all three types of cards to increase the difficulty of copying or counterfeiting them.

information and transactions—to authenticate the cards and ensure the data on the cards have not been altered.[20]

[20]Encryption is the process of transforming ordinary information, commonly referred to as plaintext, into code form. Conversely, decryption is the process of transforming coded information into plaintext. Smart cards that are used in conjunction with PKI involve the use of public and private "keys." To authenticate the card using PKI, the card transmits information encrypted with a private key. The encrypted information can only be decrypted with a corresponding public key. Decrypting the information with the public key authenticates the identity of the card because the public key will only decrypt information that has been encrypted using the card's private key. The public key is made freely available to any entities that wish to be able to authenticate the card. For more information about PKI, see GAO, *Border Security: Better Usage of Electronic Passport Security Features Could Improve Fraud Detection*, GAO-10-96 (Washington, D.C.: Jan. 22, 2010).

Figure 1: Comparison of the Functions and Technical Capabilities of Electronically Readable Cards for Potential Uses in Medicare

Authentication	Smart Card[a]	Magnetic Stripe	Bar Code
Resistance to counterfeiting or copying[b]	High	Low	Low
Ability to be used with public key infrastructure to ensure card authenticity[c]	Yes	No	No
Use with second authentication factor	Yes	Yes	Yes
On-card vertification of second authentication factor	Yes	No	No
Storing and exchanging medical information	Smart Card[a]	Magnetic Stripe	Bar Code
Storage capacity for medical information[d]	Medium	Low	Low
Ability to secure stored data[e]	High	Low	Low
Ability to limit access to information on the cards	Yes	No	No
Conveying identity and insurance information	Smart Card	Magnetic Stripe	Bar Code
Sufficient storage capacity to store identity and insurance information	Yes	Yes	Yes

Source: GAO analysis of industry, academic, and federal agency documents. | GAO-15-319

[a]The capabilities of smart cards depend on the particular chip used, and not all chips have all of these capabilities.

[b]This refers to the difficulty of counterfeiting or copying the electronically readable features or information on the cards. Physical security features, such as holograms or watermarks, can be used on all three types of cards to increase the difficulty of copying or counterfeiting the cards. For the purposes of this analysis, the high and low ratings are relative among the three types of cards and are based on capabilities that make the electronically readable features of the cards harder to recreate and can restrict access to information on the cards.

[c]Smart cards that are used in conjunction with public key infrastructure involve the use of public and private "keys." To authenticate the card using public key infrastructure, the card transmits information encrypted with a private key. The encrypted information can only be decrypted with a corresponding public key. Decrypting the information with the public key authenticates the identity of the card because the public key will only decrypt information that has been encrypted using the card's private key. The public key is made freely available to any entities that wish to be able to authenticate the card.

[d]The amount of storage capacity needed to store medical information on a card would depend on the content and file sizes of the information on the card. For this analysis, we defined low storage capacity as the ability to store a very limited amount of information; medium as the ability to store many pages worth of textual information, but not large data files; and high as the ability to store large data files. Although smart cards would be able to store significantly more medical information than cards with magnetic stripes and barcodes, it is unlikely that they would be able to store all of a beneficiary's medical records or larger file size medical records, such as medical images.

[e]For this analysis, the high and low ratings are relative among the three types of cards and are based on the presence of multiple electronically readable card capabilities that can restrict access to information on the cards.

All three types of cards could be used in conjunction with other authentication factors, such as a PIN or biometric information, to achieve a higher level of authentication. However, only smart cards are capable of performing on-card verification of other authentication factors. For example, smart cards can verify whether a user provides a correct PIN or can confirm a fingerprint match, without being connected to a separate IT system. Cards with magnetic stripes and barcodes cannot perform such on-card verification, and require a connection to a separate IT system to verify PINs or biometric information.

We also determined that using electronically readable cards to store and exchange medical information would likely require the use of smart cards given their storage capacity and security features. Smart cards have a significantly greater storage capacity than magnetic stripe and bar code cards, and would be able to store more extensive medical information on the cards.[21] However, the storage on smart cards is limited, so it is unlikely that the cards would be able to store all of a beneficiary's medical records or medical records of a larger file size, such as medical images. In addition, smart cards could better secure confidential information, including individually identifiable health information subject to protection under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[22] Smart cards can be implemented with PKI to perform public key encryption and authentication to secure and securely transmit any

[21]Depending on the chip, smart cards can store up to 256 kilobytes of data, while magnetic stripe cards can store up to 2 kilobytes and bar code cards can store up to 3 kilobytes.

[22]Pub. L. No. 104-191, Title II, Subtitle F, 110 Stat. 1936, 2021 (codified, as amended, at 42 U.S.C. ch. 7., subch. XI, pt. C., §§ 1320d et seq.).

medical information on the card.[23] Smart cards' ability to perform on-card verification can also be used to limit access to information on the cards to better ensure that information is not accessed inappropriately. For example, beneficiaries could be required to enter a PIN for providers to access medical information on the card, while access to nonsensitive information could be allowed without beneficiaries entering a PIN.

Our analysis also found that any of the three types of electronically readable cards could be used to convey beneficiary identity and insurance information to providers. Each type of card has adequate storage capacity to contain such information, and storing this type of information may not require cards with processing capabilities or security features. If beneficiary SSNs continue to serve as the main component of Medicare numbers, cards with security features would be needed to reduce the risk of identity theft.

The Use of Electronically Readable Cards Would Provide Limited Benefits for Reducing Fraud, but Could Aid Administrative Processes

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. Using electronically readable cards to store and exchange medical records is not part of current federal efforts to facilitate health information exchange and would likely present challenges. Using electronically readable cards to convey identity and insurance information to auto-populate and retrieve information from provider IT systems could reduce errors in the reimbursement process and improve medical record keeping.

[23]Although information stored on magnetic stripe and bar code cards can be encrypted before being written onto the cards, the cards cannot perform encryption and decryption functions, and any encrypted information on the cards must be encrypted and decrypted using separate IT systems.

Authentication Could Make Certain Types of Fraud More Difficult, but Paying Claims for Services When Cards Were Not Used Would Limit Effect on Fraud

Using electronically readable cards to authenticate beneficiary and provider presence at the point of care could potentially limit certain types of Medicare fraud. However, we could not determine the extent to which authenticating beneficiaries and providers at the point of care could limit fraud because there is no reliable estimate of the extent or total dollar value associated with specific types of Medicare fraud schemes. Stakeholders told us that authenticating beneficiaries at the point of care could potentially limit schemes in which Medicare providers misuse beneficiary Medicare numbers to bill fraudulently for services. In such schemes, providers use beneficiary Medicare numbers to bill on their behalf without having ever seen or rendered care to the beneficiaries. As of May 2014, CMS was aware of 284,000 Medicare beneficiary numbers that had been compromised and potentially used to submit fraudulent claims.[24] Stakeholders also told us that authenticating providers at the point of care could potentially limit fraud schemes in which individuals or companies misuse an unknowing provider's Medicare enrollment information to submit claims and divert stolen reimbursements.

Adding another authentication factor, such as a PIN or a biometric factor, to a beneficiary's card also could limit the potential for individuals to use a stolen Medicare card to obtain care or bill for services. For example, individuals attempting to use a stolen card could not pose as a beneficiary or bill for services on behalf of a beneficiary without knowing the beneficiary's PIN. Beneficiaries would still be able to lend their card to others and tell them their PIN, though replicating a biometric factor would be more difficult.

Despite the potential to curtail certain types of Medicare fraud, using beneficiary cards for authentication at the point of care would have limited effect since CMS has stated that it would continue to pay claims regardless of whether a card was used. CMS officials and stakeholders

[24]Not all compromised beneficiary numbers have necessarily been used for potentially fraudulent billing. For example, some numbers may be considered compromised because of reported security breaches. In 2012, the HHS Office of Inspector General reported on challenges faced by CMS in responding to compromised Medicare numbers. See Department of Health and Human Services Office of Inspector General, *CMS Response to Breaches and Medical Identity Theft*, OEI-02-10-00040 (Washington, D.C.: October 2012). According to CMS officials, they are limited in their ability to address compromised numbers because the agency currently cannot issue beneficiaries new Medicare numbers since the numbers are based on the SSN. CMS officials further stated that using an electronically readable Medicare card would not help in addressing this issue.

told us that requiring cards to be used would not be feasible because of concerns that doing so would limit beneficiaries' access to care. Specifically, CMS officials told us the agency would not want to make access to Medicare benefits dependent on beneficiaries having their card at the point of care. According to CMS officials and stakeholders, there are legitimate reasons why a card may not be present at the point of care, such as when beneficiaries or providers forget their cards or during a medical emergency. Because CMS has indicated that it would still process and pay for these claims, providers submitting potentially fraudulent claims could simply not use the cards at the point of care. Some stakeholders noted that CMS could mitigate the risk of paying claims in which cards are not used by using its Fraud Prevention System or other IT systems to identify and investigate providers with suspicious billing patterns related to card use. For example, such systems could identify providers that submit an abnormally high percentage of claims in which cards are not used, which could be indicative of claims for beneficiaries who were never seen or rendered care. However, CMS officials noted that they already use their IT systems to identify providers that bill for services for beneficiaries who were never seen or rendered care. For example, CMS analyzes billing patterns to identify and conduct postpayment investigations into providers that submit an abnormal number of claims for beneficiaries with known compromised numbers.

According to stakeholders, the use of electronically readable beneficiary cards would also have little effect on many other potentially fraudulent and abusive provider billing practices. For example, use of the cards would not prevent providers from mischaracterizing services, billing for medically unnecessary services, or adding a service that was not provided to a claim for otherwise legitimate services because such fraud does not involve issues related to authentication. Instead, these types of fraud typically involve providers that wrongly bill Medicare for the care provided, or misrepresent the level or nature of the care provided. The use of electronically readable beneficiary and provider cards would also have little effect on preventing fraud that involves collusion between providers and beneficiaries because complicit beneficiaries, including those who receive kickbacks, would likely allow their cards to be misused.

Examples of Common Medicare Fraud Schemes That Resulted in Convictions

- **Provider billed for services for beneficiaries that were never seen or rendered care:** Two owners of a home health agency paid kickbacks to obtain information on Medicare beneficiaries and used the information to bill for home health care services that were not actually rendered.
- **Provider billed for upcoded services:** The owner of a durable medical equipment company fraudulently billed Medicare for expensive, computerized prosthetics while providing beneficiaries with less sophisticated prosthetics.
- **Provider billed for "unbundled" services:** A doctor performing surgeries on beneficiaries billed Medicare for individual steps involved in the surgeries, rather than the entire procedure to fraudulently increase reimbursements.
- **Provider billed for noncovered services as covered services:** The owner of a medical transport company provided beneficiaries with routine, nonemergency transportation services not covered by Medicare, but billed Medicare for emergency ambulance transportation, which is covered by Medicare.
- **Provider paid or received kickbacks for beneficiary referrals for specific services, or for the purchase of goods or services that may be paid for by Medicare:** The operator of a home health agency paid illegal kickbacks to physicians to refer beneficiaries who were not homebound or who otherwise did not qualify for home health services, resulting in fraudulent Medicare billing for home health services.
- **Beneficiary solicited or received kickbacks to allow provider to fraudulently bill for services:** Two beneficiaries solicited and received kickbacks to serve as patients for a home health agency that fraudulently billed Medicare for physical therapy services.

Source: GAO analysis of Department of Justice press releases. | GAO-15-319

Officials we spoke with in France and Germany told us that the use of electronically readable cards has not limited certain types of fraud. Officials from provider organizations and an insurance organization in Germany told us that the use of beneficiary cards does not prevent providers from fraudulently adding services that they never provided onto otherwise legitimate claims. In addition, officials from France noted that certain elderly or infirm beneficiaries may need to rely on providers to maintain custody of and use their cards, and there had been instances of providers and caretakers misusing beneficiary cards in such cases. For example, officials from an insurance organization in France noted that nurses and caretakers of elderly patients have stolen patient cards and allowed other providers to misuse them.

Finally, there are also concerns that the use of an electronically readable card could introduce new types of fraud and ways for individuals to illegally access Medicare beneficiary data. For example, CMS officials said that malicious software written onto an electronically readable card could be used to compromise provider IT systems. In addition, CMS officials noted that individuals could illicitly access beneficiary information through "card skimming."[25] However, Medicare beneficiary data in provider IT systems may already be vulnerable to illegal access and use.[26]

[25]Card skimming is the unauthorized reading and collection of data stored on electronically readable cards. Because of their ability to secure stored data, smart cards may be less vulnerable to card skimming.

[26]For example, between September 2009 and March 2012, HHS's Office for Civil Rights identified over 400 reports of provider data breaches involving protected health information that each affected more than 500 individuals. See GAO-12-831.

Exchanging Medical Information with Electronically Readable Cards Is Not Part of Current Health Information Exchange Initiatives, and Would Likely Present Challenges

Using electronically readable cards to store and exchange beneficiary medical information is not part of current federal efforts to facilitate electronic health information exchange and would likely present challenges. To help improve health care quality, efficiency, and patient safety, the Medicare EHR Incentive Program provides financial incentives for Medicare providers to increase the use of EHR technology to, among other things, exchange patient medical information electronically with other providers.[27] In addition, ONC has funded health information exchange organizations that provide support to facilitate the electronic exchange of health information between providers. These and other ongoing federal health information exchange programs aim to increase the connections and exchanges of medical information directly between provider EHR systems so that patient medical information is available where and when it is needed. None of these existing programs include the use of electronically readable cards to store or exchange medical information. Using electronically readable cards to store and exchange beneficiary medical information would introduce an additional medium to supplement health information exchange among EHR systems, with beneficiaries serving as intermediaries in the exchange.

Stakeholders noted that implementing another medium, such as a card, that stores beneficiary medical information outside of provider EHR systems could lead to inconsistencies with provider records. Stakeholders, including a health care IT vendor and a provider organization, stated that storing beneficiary medical information on beneficiary cards in addition to EHR systems could lead to problems with ensuring that medical information is synchronized and current. For example, beneficiaries who have laboratory tests performed after medical encounters would not have a means to upload the results to their cards before visiting their providers again, leading to cards that are not synchronized with provider records.

[27]See the Health Information Technology for Economic and Clinical Health Act (HITECH Act). Pub. L. No. 111-5, §§ 4101, 4102, 123 Stat. 115, 467, 477 (2009) (pertinent provisions codified as amended at 42 U.S.C. §§ 1395w-4(o), 1395ww(n)). Participants in the Medicare EHR Incentive Program must use certified EHR technology that meets certain criteria established by ONC and demonstrate “meaningful use” of EHR technology. For more information, see GAO, *Electronic Health Record Programs: Participation Has Increased, but Action Needed to Achieve Goals, Including Improved Quality of Care*, GAO-14-207 (Washington, D.C.: Mar. 6, 2014).

Several stakeholders also stated that using electronically readable cards to store and exchange medical information would likely face similar interoperability issues encountered by federal health exchange programs and providers implementing EHR systems.[28] Information that is electronically exchanged among providers must adhere to the same standards in order to be interpreted and used in EHRs. We previously found that insufficient standards for electronic health information exchange have been cited by providers and other stakeholders as a key challenge for health information exchange.[29] For example, we found that insufficient standards for classifying and coding patient allergy information in EHRs could potentially limit providers' ability to exchange and use such information. The use of electronically readable cards would involve exchanging medical information through an additional medium, but it would also be subject to the same interoperability issues that currently limit exchange.

Despite potential challenges using electronically readable cards to store and exchange medical information, several stakeholders noted that adding patient health information to an electronically readable card may have benefits such as better health outcomes in emergency medical situations. For example, a beneficiary card containing medical information could be used by an emergency care provider to access important information that might otherwise be unknown, such as beneficiary allergy information.

One potential benefit of electronically readable provider cards is that they could provide an option to authenticate providers accessing EHR systems, especially for remote online access.[30] EHR systems that store patient medical information can be accessed from places outside the clinical setting, and there are concerns regarding the current level of identity authentication to ensure that only authorized providers are accessing the systems remotely. Although no determinations have been

[28]Interoperability is the ability of two or more systems or components to exchange information and to use the information that has been exchanged.

[29]See GAO, *Electronic Health Records: HHS Strategy to Address Information Exchange Challenges Lacks Specific Prioritized Actions and Milestones*, GAO-14-242 (Washington, D.C.: Mar. 24, 2014).

[30]"Remote" access, for example, could include accessing an EHR system from outside of a provider organization's private network.

made regarding what specific authentication practices are needed, or what types of technology should be used for remote access, an HHS advisory committee has recommended that the Medicare EHR program implement rules regarding how providers should be authenticated when remotely accessing EHR systems.[31] According to an electronically readable card industry organization, electronically readable cards could be used to authenticate providers remotely accessing EHR systems.

Using Electronically Readable Cards to Convey Beneficiary Identity and Insurance Information Could Reduce Reimbursement Errors and Improve Medical Record Keeping

Using electronically readable cards to convey identity and insurance information to auto-populate and retrieve information from provider IT systems could reduce errors in the reimbursement process and improve medical record keeping and health information exchange. Many providers currently capture identity and insurance information by photocopying insurance cards and manually entering beneficiary information into their IT systems, which can lead to data entry errors. In addition, providers have different practices for entering beneficiary names, such as different practices for recording names with apostrophes and hyphens, or may use beneficiary nicknames, leading to possible naming inconsistencies for a single individual. The failure to initially collect accurate beneficiary identity and insurance information when providers enter patient information into their IT systems, or retrieve information on existing beneficiaries, can compromise subsequent administrative processes.

According to stakeholders, using an electronically readable card to standardize the process of collecting beneficiary identity and insurance information could help reduce errors in the reimbursement process. When beneficiaries' identity or insurance information is inaccurate, insurers reject claims for those beneficiaries. Providers then must determine why

[31]The HHS Health IT Policy Committee—a federal advisory committee—recommended multifactor authentication for remote EHR access, and also recommended that CMS continue to monitor any and all technology options to authenticate individuals and to monitor and re-assess authentication practices. See Department of Health and Human Services, *Health IT Policy Committee letter to the National Coordinator for Health Information Technology* (Sept. 26, 2012), accessed Sept. 26, 2014, http://www.healthit.gov/sites/faca/files/transmittal_092512_pstt_recommendations_provider_authentication.pdf. Although not specific to remote EHR system access, the White House has an initiative, the National Strategy for Trusted Identities in Cyberspace, to encourage the development of technologies and practices to improve online identity authentication. Currently, the most common practice for online identity authentication is the use of usernames and passwords, which provide a relatively low level of identity authentication and security.

the claims have been rejected, and reimbursements are delayed until issues with the claims are addressed and the claims are resubmitted. Once any issues are addressed, insurers reprocess resubmitted claims. Based on data provided by CMS, we found that up to 44 percent of the more than 70 million Medicare claims that CMS rejected between January 1, 2014, and September 29, 2014, may have been rejected because of invalid or incorrect beneficiary identity and insurance information that could be obtained from beneficiaries' Medicare cards.[32] In addition, HHS has cited an industry study indicating that, industrywide, a significant percentage of denied health insurance claims are due to providers submitting incorrect patient information to insurers.[33] However, CMS officials stated that using electronically readable cards may not necessarily reduce claim rejections because providers may still obtain beneficiary information in other ways, including over the telephone or paper forms that have been filled out by beneficiaries.

Stakeholders also told us that problems with collecting beneficiary information can lead to the creation of medical records that are not linked accurately to beneficiaries or records that are linked to the wrong individual, which can lead to clinical inefficiencies and potentially compromise patient safety.[34] For example, problems collecting beneficiary information can prevent providers from retrieving existing beneficiary records from their IT systems, leading providers to create duplicate

[32]The percentage of claim rejections due to invalid or incorrect beneficiary identity and insurance information that could be obtained from beneficiaries' Medicare cards may be lower than 44 percent. The data provided by CMS included a data field to indicate claims that were rejected due to an invalid or incorrect beneficiary name, Medicare number, gender, or date of birth. Although name, Medicare number, and gender are printed on beneficiaries' Medicare cards, date of birth is not, and the data did not break out rejections that were due to invalid or incorrect date of birth. Claim rejections as a result of an invalid or incorrect date of birth would not constitute rejections as a result of invalid or incorrect information obtained from beneficiaries' Medicare cards.

[33]Operating Rules for Health Care Claim Status Transactions, 76 Fed. Reg. 40,458, 40,477 (Jul 8, 2011) (preamble discussion pertaining to cost benefit studies considered for regulatory impact analysis).

[34]In 2011, the HHS Health IT Policy Committee recommended the implementation of standardized formats for collecting beneficiary identity information for electronic health records. See Department of Health and Human Services, Health IT Policy Committee letter to the National Coordinator for Health Information Technology (Feb. 8, 2011), accessed Dec. 5, 2014, http://www.healthit.gov/sites/faca/files/hitpc-transmittal-letter-priv-sectigerteam-020211.pdf.

medical record files that are not matched to existing beneficiary records.[35] Medical records that are not accurately linked to beneficiaries can compromise a provider's ability to make clinical decisions based on complete and accurate medical records, which can lead to repeat and unnecessary medical tests and services, and adverse events, such as adverse drug interactions.

Furthermore, inaccurate and inconsistent beneficiary records can also limit electronic health information exchange by limiting the ability to match records among providers. We previously found that difficulty matching beneficiaries to their health records has been a key challenge for electronic health information exchange, and this can lead to beneficiaries being matched to the wrong set of records, and to providers needing to match records manually.[36]

Health care entities that have used electronically readable cards told us that the cards have helped with administrative processes. Officials from provider organizations and federal agencies in France and Germany told us that their use of electronically readable cards to convey beneficiary identity and insurance information has helped improve their reimbursement processes by preventing errors associated with manual data entry. Certain provider networks in the United States that have issued electronically readable cards to patients have reported that their cards have helped with medical record keeping. VA issued an electronically readable magnetic stripe card to its beneficiaries that is used to access beneficiary records from VA's EHR system.[37] In addition, an official from a hospital-based integrated health system told us that the health system's issuance of patient smart cards has greatly reduced medical record keeping errors by eliminating the creation of duplicate patient medical records. According to some stakeholders, however,

[35]ONC released a report in 2014 that reviewed issues and provider best practices related to patient identification and matching patient records. See Audacious Inquiry, LLC, *Patient Identification and Matching Final Report*, report prepared at the request of the Office of the National Coordinator for Health Information Technology (Baltimore, Md.: Feb. 7, 2014), accessed on Jan. 14, 2015, http://www.healthit.gov/sites/default/files/patient_identification_matching_final_report.pdf.

[36]GAO-14-242.

[37]VA also recently issued new paper cards to certain veterans to obtain care outside of VA facilities. See the Veterans Access, Choice and Accountability Act of 2014, Pub. L. No. 113-146, § 101(f),128 Stat. 1754, 1760 (codified at 38 U.S.C. § 1701 note).

providers are increasingly collecting and ensuring the accuracy of beneficiary identity and insurance information prior to appointments, through either telephone conversations or online portals to preregister for appointments. This practice of ensuring the accuracy of beneficiary information prior to appointments may limit the possible benefits of using electronically readable cards to convey information at the point of care.

CMS and Providers Could Face Challenges Implementing Cards for Authentication, but Conveying Identity and Insurance Information Would Be Less Complex

CMS would need to update its claims processing systems to use electronically readable cards to authenticate beneficiary and provider presence at the point of care, while using the cards to convey beneficiary identity and insurance information might not require CMS to make IT updates. Similarly, using electronically readable cards for authentication would require updates to CMS's current card management processes, while using the cards to convey beneficiary identity and insurance might not. For all potential uses of electronically readable cards, Medicare providers could incur costs and face challenges updating their IT systems to read and use information from the cards.

Authentication Would Involve Costs and Updates to CMS's IT Systems, but Conveying Identity and Insurance Information Might Not Require Updates

Using electronically readable cards to authenticate beneficiaries and providers would require updates to CMS's claims processing systems to verify that the cards were swiped at the point of care. CMS officials told us they have not fully studied the specific IT updates that would be needed to the claims processing system and could not provide an estimate of costs associated with implementing any updates. However, they noted that any IT updates would necessitate additional funding and time to implement, and could involve IT challenges.

Based on our research, we identified two options for how CMS could verify that the cards were swiped by beneficiaries and providers at the point of care.

- The first option is based on proposals from an HHS advisory organization and a smart card industry organization. When beneficiaries and providers swipe their cards, CMS's IT systems would generate and transmit unique transaction codes to providers.

Providers would include the transaction codes on their claims. When processing claims, CMS would match the original transaction codes generated by CMS's IT systems with the codes on submitted claims.[38] For this option, CMS officials told us that they would need to implement an IT system to collect and store data on the transaction codes and build electronic connections with existing claims processing systems to match the codes with submitted claims.

- The second option is based on the processes used in a CMS pilot program.[39] When beneficiaries and providers swipe their cards, information about the card transaction—such as the date of the transaction and the beneficiary Medicare number and provider NPI associated with the cards—would be sent to CMS. CMS would match this information about the card transaction with information on the claims submitted by the providers. According to officials, this option would similarly involve implementing an IT system to collect and store data on the card transactions and connecting the system with existing claims processing systems to match information about the transactions with submitted claims.[40]

[38]An HHS advisory organization, the Workgroup for Electronic Data Interchange (WEDI), issued a white paper examining the potential for health care insurers to authenticate beneficiaries' presence at the point of care through such transaction codes. See Workgroup for Electronic Data Interchange, *Secure Patient Identification: Feasibility of a Security Role for Subscriber ID Cards* (Reston, Va.: Nov. 3, 2014), accessed Jan. 2, 2015, https://wedi.org/docs/resources/secure-patient-identification-research-paper.pdf?sfvrsn=0. A smart card industry organization has similarly noted that Medicare could use smart cards to authenticate beneficiaries and providers at the point of care through such transaction codes.

[39]In 2011 and 2012, CMS conducted a pilot program in which physicians and suppliers were issued electronically readable cards that they swiped when referring or fulfilling medical supply orders. When swiping the cards, they entered the last four digits of the beneficiary's Medicare number into credit card readers. CMS used information from the card transactions, including the date and beneficiary Medicare numbers, to match the transactions to submitted claims. The pilot only studied the ability to match card transactions with submitted claims, and did not involve any changes to claims processing systems or the adjudication process. CMS officials told us that they were not able to assess any program integrity effect from use of the cards due to low provider participation in the pilot.

[40]In addition to the two options we identified, we also identified proposals to use smart cards to "electronically sign" claims, though it is likely not feasible that beneficiary cards could be used to do so. Generally, claims are generated after care has been provided, preventing beneficiaries from electronically signing claims with a smart card when they are present at the point of care.

CMS officials told us that verifying that beneficiary and provider cards were swiped by including new content on claims—such as unique transaction codes—would be problematic. Doing so would involve changes to industrywide standards for claim submission and the way in which CMS's IT systems receive submitted claims. These industrywide standards govern the data content and format for electronic health care transactions, including claim submission.[41] Adding new content to claims, such as a field for a transaction code, would require CMS to seek changes to existing claim standards with the standard-setting body responsible for overseeing the data content and format for electronic health care transactions. Officials told us that requesting and having such changes approved could take several years.[42] CMS officials further noted that the IT infrastructure that CMS developed to accept electronic claim submissions was built to accept claims based on current standards and would need to be updated to accept any new content fields. However, under the second option, verifying that the cards were swiped by matching information about the card transaction—such as the date and beneficiary and provider identification information—with information on the claims submitted would not involve additional content on claims because CMS would be matching the card transactions with information currently included on claims.

In addition to updates to CMS's claims processing systems, based on our analysis, CMS would need to implement a PKI system to use smart cards to achieve a higher level of authentication for beneficiaries and providers or to secure any medical information on the cards. Implementing a PKI system for smart cards involves the creation, issuance, and management of public and private keys. The keys are used to authenticate the cards and to secure information stored on and transmitted by the cards. As we have previously reported, implementing a PKI system is a significant undertaking.[43] However, officials from the General Services

[41]HIPAA, as amended, requires the adoption of standards and data elements for certain health-related transactions, to enable health information to be exchanged electronically with as much uniformity in the standards as possible. Pub. L. No. 104-191 § 262(a), 110 Stat. 2024 as amended by Pub. L. No. 111-148, § 10109(a), 124 Stat. 915 (codified at 42 U.S.C. § 1320d-2).

[42]According to an official at WEDI, CMS could potentially include a transaction code on claims as part of a pilot program without changes to industrywide standards for claims, though any permanent use of such codes would require changes.

[43]See GAO, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO-01-277 (Washington, D.C.: Feb. 26, 2001).

Administration, which manages a program that offers PKI services to federal agencies, told us that CMS could leverage such services to use PKI for electronically readable Medicare cards. CMS officials stated that CMS has not studied this issue and said they could not provide any cost estimates for using PKI for electronically readable Medicare cards.

In contrast to using electronically readable cards for authentication, using the cards to convey beneficiary identity and insurance information may not require updates to CMS's IT systems. Using the cards to convey such information primarily involves transferring information from the card to provider IT systems, as opposed to interacting with CMS IT systems. However, CMS officials said if any additional identity or insurance information is put on an electronically readable card that requires changes to the content or formatting of claims, CMS would have to update its claims processing systems.[44]

Authentication Would Require New Card Management Processes and Could Present Challenges, while Conveying Identity and Insurance Information Might Not

CMS would need to update and obtain additional resources for its current card management processes to use electronically readable cards to achieve a higher level of authentication for beneficiaries and providers. Card management processes involve procedures for enrollment, issuing cards, replacing cards, updating information on cards, deactivating cards, and addressing cardholder issues, among other processes; and developing standards and procedures for card use. Medicare currently does not issue cards to providers, and therefore CMS would need to implement a new program to issue and manage provider cards and to develop standards and procedures for card use.

In addition, we found that new standards and procedures for card use would likely need to be developed to implement electronically readable cards to authenticate beneficiaries and providers. Proponents have suggested that NIST standards for electronically readable cards could be used to implement such cards for Medicare. However, these standards generally apply to the issuance and use of smart cards by federal employees and contractors for accessing computers and physical locations, and we found that the application of such standards could present logistical challenges for Medicare and could entail changes to

[44]In particular, implementing electronically readable cards that convey a new beneficiary identifier, as opposed to the current Medicare number, would require significant changes to CMS's IT systems. See GAO-12-831.

current Medicare card management practices. For example, NIST standards involve procedures for verifying the identities of individuals before they are issued cards and, among other requirements, require potential cardholders to appear in person before being issued a card.[45] Medicare does not require beneficiaries to appear in person to be enrolled in the program and issued cards. Doing so could present barriers to beneficiary enrollment and could present logistical challenges, given that Medicare covered approximately 54 million beneficiaries in 2014 and CMS does not have an infrastructure in place to meet beneficiaries in person. Additionally, to use the cards with a PKI system, CMS would need to implement processes to update and reissue beneficiary cards as needed to meet security requirements. Currently, the NIST standards require cards to be reissued every 6 years to update the PKI keys on the cards. Reissuing cards on a regular basis would likely require the implementation of new card management processes and additional resources for CMS. As of now, CMS only reissues cards if they are reported as lost, stolen, or damaged, or if there is a change to beneficiary information, such as a name change.

CMS would face additional card management challenges and practical concerns to use electronically readable cards in conjunction with a PIN or biometric information. According to CMS officials, implementing PINs or biometrics would come with large costs and would involve significant changes for CMS and beneficiaries. To use PINs, CMS would need to implement processes for creating, managing, and verifying them. CMS officials and other stakeholders also noted that certain Medicare beneficiaries, especially those with cognitive impairments, may not be able to remember their PINs. Officials we spoke with in France told us that they decided not to have beneficiaries use PINs with their cards after a pilot project found that some beneficiaries had difficulties remembering them. In terms of using biometrics, CMS officials and other stakeholders expressed concerns regarding beneficiaries' willingness to provide biometric information due to privacy considerations and the logistics involved in collecting such information from beneficiaries. Both France and Germany are currently issuing cards that include photographs of beneficiaries, and officials from both countries told us that they experienced difficulties collecting them. Both countries allow beneficiaries

[45]National Institute of Standards and Technology, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* Federal Information Processing Standards Publication 201-2 (Gaithersburg, Md.: August 2013).

to submit their photographs by mail, and Germany allows beneficiaries to submit their photographs online.[46] Officials from Germany noted that because the pictures are not taken in person, there are few controls in place to ensure that beneficiaries submit a representative photograph of themselves. VA includes a photograph of the veteran on its cards, which it generally obtains in person at local medical centers. CMS does not have an infrastructure like VA to take photographs of Medicare beneficiaries.

CMS would need to implement processes for securing information on electronically readable cards to use them to store and exchange beneficiary medical information. CMS and ONC officials and other stakeholders expressed concerns about storing individually identifiable health information on the cards and told us that beneficiaries would likely be sensitive to having their medical information on the cards, so the security processes in place to protect this information would need to be rigorous. In particular, processes would be needed for accessing and writing information onto the cards to ensure that beneficiaries could control who could view stored information and to ensure that only legitimate providers are able to access information from or write information onto the cards.

In contrast with using electronically readable cards for authentication or to store and exchange beneficiary medical information, we found that CMS would not necessarily need to make changes to current standards and procedures for the cards to electronically convey beneficiary identity and insurance information. The cards would not be used in a significantly different way than they are now—to convey information that providers use to verify beneficiary eligibility and to submit claims—and accordingly, little would change other than the type of card CMS issues. Instead of a paper card, CMS would need to produce and issue an electronically readable card.[47] Although the use of electronically readable health insurance cards in the United States has been limited, there are existing industry standards for using such cards to convey identity and insurance information. An HHS advisory organization, the Workgroup for Electronic

[46]Officials in France told us that they are planning to allow beneficiaries to submit their photographs online.

[47]CMS officials told us that producing and issuing an electronically readable Medicare card could be more costly than producing and issuing the current paper card.

Data Interchange (WEDI), has issued formatting and terminology standards for using electronically readable cards that could be applied to electronically readable Medicare cards.[48]

CMS officials also noted that the implementation of electronically readable cards would require beneficiary and provider education and outreach regarding the new cards and any associated changes related to how the cards are used. For example, CMS would have to disseminate information on the different functions and features of any card and information on what to do if the electronically readable functions of the card are not working. For cases where IT systems malfunctioned or IT access was an issue, CMS officials stated the agency would need to have support services in place for providers and beneficiaries, and paper back-up options.

Providers Could Incur Costs and Face Challenges Updating Their IT Systems to Implement Electronically Readable Cards

For all potential uses of electronically readable cards, Medicare providers could incur costs and face challenges updating their IT systems to read and use information from the cards. For providers to use electronically readable cards, they would need to have hardware, such as card readers, to read information from the cards. According to stakeholders, including provider organizations, health care IT, transaction standards, billing, and management organizations, and health care IT vendors, in general, providers would also need to update their existing IT system software to use the information on cards. For example, to use electronically readable cards to store and exchange beneficiary medical information, providers' EHR systems would need to be updated to be able to read and use the medical information on the cards.

Generally, providers would have to update their existing IT systems with a type of software called middleware to interact with and use information from electronically readable cards, and such updates could involve significant challenges.[49] According to stakeholders we spoke with, provider IT systems, including billing systems and EHRs, vary widely and often are customized to meet the needs of individual providers. While

[48]See Workgroup for Electronic Data Interchange, *Health Identification Card Implementation Guide* (Reston, Va.: Apr. 28, 2011).

[49]Middleware is software that connects two otherwise separate IT applications and allows the applications to exchange and use information from the other application.

some providers have a single, integrated IT system for billing, tracking patient medical information, and other administrative applications, other providers have individual systems for each application, such as practice management, billing, and EHR systems. Because of the variety and customization of systems in place, providers may need to implement uniquely developed middleware for each software system the cards would interact with to ensure that their IT systems could read and use information from the cards.

Updating provider IT systems to use electronically readable cards for beneficiary and provider authentication by including transaction codes on claims could prove particularly challenging. To do so, the cards would need to be able to interact with provider IT systems used for billing so that the systems could incorporate the transaction codes generated by the cards onto provider claim forms. Stakeholders told us that current provider IT systems are not designed to interact with electronically readable cards to incorporate transaction codes generated by the cards onto claims.[50] Additionally, they said that provider billing practices vary widely, which presents challenges for developing standard ways to update provider IT systems to be able to perform this function. For example, some providers have IT systems capable of directly billing CMS, while others use IT systems that electronically transmit clinical encounter information to third-party billers, who generate and submit claims to CMS. Some providers do not use IT systems, and submit paper claims or clinical encounter information to clearinghouses, which convert the claims into electronic format and submit them to CMS.

If information about the card transaction is sent directly to CMS—and no transaction codes are included on claims—providers would not necessarily need to update their existing IT software. In CMS's 2011 and 2012 electronically readable card pilot program, participating physicians and suppliers did not need to update their IT systems, as they used magnetic stripe cards and sent the information to CMS using existing credit card readers and networks. However, if CMS used smart cards with PKI for authentication rather than magnetic stripe cards and credit card readers, providers would likely need to purchase card readers and software capable of authenticating the cards.

[50]The WEDI white paper proposal to authenticate beneficiaries at the point of care proposes allowing providers to manually enter card transaction codes into their IT systems so that the cards would not necessarily need to interact with current provider IT systems.

While some provider IT systems would need to be updated with middleware to be able to use beneficiary identity and insurance information conveyed by electronically readable cards, some provider systems already have this capability. One vendor noted that its IT systems are capable of using beneficiary identity and insurance information from cards that comply with WEDI electronically readable card standards to auto-populate and retrieve information from their IT systems. In addition, an insurer that issues electronically readable cards that comply with WEDI standards told us that there are providers that currently use its cards to auto-populate information into their IT systems, though this insurer could not estimate the percentage of providers who do so.

In addition to updating IT systems, CMS officials and stakeholders also expressed concerns regarding how using electronically readable cards to authenticate providers at the point of care would be incorporated into provider workflows. During the pilot program conducted by CMS, participating providers told CMS that using the cards was an administrative burden that required changes to their workflows. Stakeholders noted that it might not be practical for providers to swipe the cards during the course of providing care and that the cards might instead be used by administrative or billing staff. However, having administrative staff use provider cards could create complexity in terms of card use and limits the ability of the card to be used to authenticate provider presence at the point of care. For some providers, administrative and billing processes might not take place at the same location where care is provided.

Stakeholders also expressed logistical concerns regarding when and how beneficiary and provider cards would be swiped at the point of care. At larger provider facilities, such as hospitals, having beneficiaries and providers swipe their cards at the point of care might require providers to deploy many card readers within a single facility. Additionally, stakeholders expressed concerns regarding how the cards would be used when multiple providers provide care during a single medical encounter. For example, a beneficiary experiencing a medical emergency may be provided care by an ambulance company, hospital, and attending physicians. With each provider submitting its own claim for reimbursement, it raises questions regarding how a single swipe of the beneficiary's card would be matched to each of the claims submitted by the providers. Further, stakeholders raised questions regarding how the cards would be used by providers that may have little contact with beneficiaries, such as laboratories.

Many stakeholders also cited potential challenges encouraging providers to incur costs to purchase hardware and update their IT systems to use the cards, especially given existing CMS IT requirements. Officials at CMS and ONC, along with stakeholders, noted that Medicare providers are already investing resources, and facing IT challenges, to meet Medicare EHR Incentive Program requirements and to update their IT systems to adopt new billing codes.[51] Both France and Germany have experienced similar challenges with provider reluctance to incur costs to use electronically readable cards. According to officials from organizations we spoke with in those countries, financial subsidies to purchase hardware and update IT systems, and financial incentives for card use have been key to encouraging provider participation.

France and Germany Have Seen Successes and Challenges Implementing Electronically Readable Card Systems that Provide Lessons Learned for Medicare

France and Germany have each successfully implemented an electronically readable card system—specifically, a smart card system—on a national scale in their health care systems. The implementation of these systems provides lessons that could inform U.S. policymakers in deciding whether to adopt an electronically readable card for Medicare. Both countries' experiences demonstrate that implementation of an electronically readable card would likely be a long process and would require that competing stakeholder needs be discussed and addressed. Further, the experiences of France and Germany illustrate that after implementation, management of an electronically readable card system is a continuing and costly process.

[51]Effective October 1, 2015, CMS will require health care providers, among others, to update the billing codes that they use to indicate medical diagnoses and procedures when submitting claims. See 79 Fed. Reg. 45128, 45134 (Aug. 4, 2014) (codified at 45 C.F.R. § 162.1002). Providers will have to update their IT systems to be able to use the new codes. For additional information, see GAO, *International Classification of Diseases: CMS's Efforts to Prepare for the New Version of the Disease and Procedure Codes*, GAO-15-255 (Washington, D.C.: Jan. 28, 2015).

Implementation of Electronically Readable Cards in France and Germany Was a Lengthy Process

France and Germany's successful implementation of an electronically readable card system demonstrates that implementation of such a system on a national scale is possible. According to the organization that manages the smart card system in France, 50 million citizens, or about 76 percent of the population in France, used a beneficiary card and more than 300,000 health care providers used a health care provider card as part of a health care service in 2013. Approximately 90 percent of France's health care claims were generated by swiping both a beneficiary and a health care provider smart card. In Germany, approximately 70 million citizens, or about 85 percent of the population, used a smart card provided to beneficiaries as their health insurance card in 2014, according to government officials.[52]

The experiences of both countries also demonstrate that the implementation of an electronically readable card system can be a long process. France has had a smart card system for beneficiaries and health care providers since 1998. Officials from the organization that manages the smart card system in France told us that implementation of the system had been a slow process in part because many providers lacked the IT equipment—such as computers and printers—needed to manage their health care practices and had to obtain that equipment before being able to participate in the card system. Health care providers' resistance to voluntarily adopting and using the smart cards—despite financial incentives to do so—also contributed to the delay in implementing the smart card system fully. Fourteen years after the implementation of the smart card system in France, about 95 percent of self-employed health care providers and 18 percent of hospital-based providers in France were using health care provider cards.[53]

While the initial cards for beneficiaries were distributed in 2 to 3 years, according to French officials, issuance of an updated beneficiary card with a picture has been a slower process. French officials explained that the process of adding a photograph to the beneficiary card and issuing the updated cards has been ongoing since 2007. As of September 2014,

[52]About 12 percent of Germany's population is insured through a private insurance system that does not use these smart cards.

[53]Cour des Comptes, *Management of Public Health Teleservices Remains Insufficient* (Paris, France: February 2013). According to a French official, the use of provider cards by hospital-based providers is not mandatory in most cases.

35 percent of beneficiary cards in France being used for health care had been issued 15 years ago, according to the organization that represents health care insurers.

In 1995, Germany implemented a memory-only smart card that included information such as name, address, and insurance status.[54] The card was used to electronically transfer this information to the health care providers' IT systems. According to a report by the German auditing agency, in 2003 Germany required that a new smart card containing a microprocessor chip and with the capability to add new functionality be implemented by January 2006.[55] This report also indicated that due to technical problems and stakeholder disagreements, the initial roll out of the new cards did not occur until October 2011. By the end of 2013, almost all of the population insured through the statutory health insurance system had been issued the new cards and providers were equipped with the readers that could access information from both the new smart card and the previous memory-only smart card.[56] However, German officials told us that the full transition to the new cards will not be complete until early 2015, when beneficiaries will no longer be able to use the memory-only cards. Currently, the new smart cards are being used in the same way as the memory-only card. According to officials in Germany, new applications will be added to the new card incrementally, with the ability to update insurance information on the card being the first application and then an expansion to storing emergency care information, such as allergies and any drug interactions. Officials explained that full implementation of the new smart card—with all of the applications added—will not be completed until 2018, more than 10 years later than mandated.[57]

[54]Memory-only smart cards are smart cards with a memory chip but without processing capabilities.

[55]Bundesrechnungshof, "Audit of the Progress of the Introduction of the Electronic Health Card" (response to GAO inquiry about use of electronic health cards in Germany, Bonn, Germany, April 2014).

[56]Germany's public health insurance (commonly referred to as the statutory health insurance system) provides health insurance for most individuals through competing, not-for-profit, nongovernmental funds. Health insurance is also available through voluntary private health insurance. For more information on the French and German health care systems and their use of smart cards for health care, see app. II.

[57]As of September 2014, Germany was also in the early stages of implementing a card for providers.

The initial implementation of any new card system in Medicare could also be a lengthy process because CMS would need time to address the challenges that we described earlier. Similarly, experiences in both France and Germany have illustrated that updating a card system has the potential to be as lengthy and resource-intensive a process as the initial implementation. French officials noted that being clear about how an electronically readable card will be used and developing a system that can be easily updated are key lessons that the Medicare program should consider.

Cost Savings Achieved in France and Germany from Electronic Billing Would Not Necessarily Be Achievable for Medicare

Officials in France and Germany indicated that their governments implemented smart card systems to simplify and improve administrative processes in their health care systems. Specifically, both countries implemented a smart card as a means to move from a paper-based to an electronic billing and reimbursement process. In addition to administrative improvements, officials from both countries noted that the shift from paper to electronic billing and reimbursement has resulted in financial savings. For example, government officials in France told us that the estimated cost to process a paper claim is $2.40 per claim, while processing an electronic claim cost $0.20. Officials from France's federal auditing agency claim that the cards have been largely successful, with 93 percent of claims being submitted electronically in 2014, resulting in an estimated savings of approximately $1.5 billion per year.[58] However, according to officials from the organization that manages the beneficiary card system in France, it is difficult to isolate how much of that savings can be attributed specifically to the use of the smart cards, given that electronic billing and reimbursement could have been achieved by using technology other than an electronically readable card. German officials also reported, but did not quantify, savings associated with using smart cards to move to an electronic billing and reimbursement process.

The cost savings that France and Germany report from moving to electronic billing would not necessarily be achievable for Medicare, which has a long-standing electronic claims processing system that enables both Medicare and health care providers to process claims faster and at a lower cost. Some health care providers have been submitting claims

[58]According to officials from the French Ministry of Social Affairs, Health, and Women's Rights, the French health care system has expenditures of about $260 billion a year.

electronically since 1981, and by law Medicare has been prohibited from paying claims not submitted electronically since October 16, 2003, with limited exceptions.[59]

Addressing Stakeholder Needs Is an Important Aspect of Implementing an Electronically Readable Card System

French and German government officials told us that it is important to ensure that the competing needs of stakeholders are discussed and addressed. Officials also stated that in their experience this part of the process generally required a significant time investment and should occur prior to the decision to implement any electronically readable card. For instance, officials from provider organizations in Germany told us that health care providers took issue with what they viewed as a continued emphasis on enhancing the administrative, rather than the clinical, features of the card. Officials explained that providers and hospitals had objected to the decision to add the ability to electronically update identity and insurance information before adding the ability to store emergency care information on the new smart card. They stated that the new smart card is currently being used the same way as the memory-only smart card—to electronically transfer a beneficiary's identity and insurance information to the health care providers' IT system—which provides no new benefits for providers relative to the memory-only smart cards.

In both France and Germany, the government established independent organizations to address stakeholders' needs. For example, officials from the independent organization in Germany told us that it has seven stakeholder groups, including the National Association of Statutory Health Insurance Funds as the sole representative of all health insurance funds and six umbrella organizations representing health care providers. Officials explained that each group is assigned a different share of interest in the organization, with the stakeholder group that funds the organization holding a 50 percent share.

An organization like those established in France and Germany may not be necessary to solicit input from stakeholders in the United States. However, successful implementation of an electronically readable card system for the Medicare program would depend on stakeholder participation. An official from a health care billing and management

[59]Administrative Simplification Compliance Act, Pub. L. No. 107-105, § 3, 115 Stat. 1003, 1006 (2001) (codified at 42 U.S.C. § 1395y(a)(22),(h)).

organization told us that before implementation of any electronically readable cards for Medicare, CMS should obtain input from beneficiary and consumer advocacy groups on how the cards should be implemented. This official also told us that CMS would need to educate beneficiary and provider groups on the benefits of electronically readable cards and how to use them because beneficiary and provider buy-in would help CMS in implementing the cards. CMS officials confirmed that implementing an electronically readable card could result in a number of policy challenges that may cause resistance from provider and beneficiary advocacy organizations. CMS officials acknowledged that the agency would have to work with multiple stakeholders who have competing priorities if they were to move forward with the development and implementation of an electronically readable card.

Furthermore, implementing an electronically readable card system for Medicare would be done in a different health IT landscape than France's and Germany's. Officials in both France and Germany told us that they began implementing their systems when health care providers' use of IT systems was limited. However, in the United States, health IT is more advanced than it was in France and Germany when they first implemented the electronically readable cards. Nevertheless, according to officials from a U.S. health insurer, the disparate IT systems of health care providers in the United States will need to be modified in order to implement an electronically readable card system. French officials noted that implementation is easier when the electronically readable card system does not have to be built on top of existing hardware and software.

Card Management Processes for Electronically Readable Cards Would Need to Be Considered

Management of an electronically readable card system includes maintaining the technical infrastructure as well as continuously producing and issuing the cards. Officials from France and Germany reported that the process of managing an electronically readable card system is costly and needs to be taken into account when deciding whether to implement such a system. The independent organizations that are responsible for addressing stakeholders' needs related to the card systems in France and Germany also have an ongoing role in managing these systems. In France, an additional organization manages the health care provider card system. (See table 1.)

Table 1: Responsibilities of Organizations That Manage Smart Card Systems in France and Germany

Country	Organization	Responsibility
France	**Groupement d'Intérêt Économique SESAM-Vitale (GIE SESAM-Vitale):** Responsible for smart cards for beneficiaries	Publishes software format and content specifications; certifies software; manages systems used to transmit electronic claims, including responding to questions regarding the transmission; and produces, issues, and replaces cards
	Agence des Systèmes d'Information Partagés de Santé (ASIP Santé): Responsible for smart cards for health care providers	Manages the health care provider registry, and produces, issues, replaces, and deactivates cards
Germany	**Gematik:** Responsible for smart cards for beneficiaries[a]	Defines technical specifications and components for card system, authorizes and certifies software and hardware, and responds to questions related to the technical infrastructure

Source: GAO. | GAO-15-319

[a]As of September 2014, Germany was in the early stages of implementing a card for providers. Gematik will be responsible for managing the technical infrastructure for the provider cards as well.

Officials in both France and Germany told us that they experienced significant costs related to managing the system beyond initial implementation costs. For example, in France, government officials explained that it costs about $37 million annually to maintain the infrastructure for the beneficiary card and nearly $31 million per year in IT and human resources costs for the provider card. In addition, there are annual costs to produce, issue, and deactivate the cards. In France, for instance, the cost to produce and issue beneficiary cards is approximately $2.50 per card, and production and issuance costs for provider cards range from about $8 to $12 per card, depending on the method used to mail the card.

In Germany, the National Association of Statutory Health Insurance Funds finances the organization that manages the technical infrastructure for the card system, though the individual insurance funds are responsible for producing and issuing the beneficiary smart cards. Officials from this organization told us that they are paid about $2.40 per beneficiary annually for the development of the infrastructure. In 2014, there were approximately 70 million beneficiaries using the electronically readable cards in Germany, which equates to about $168 million in development costs.

U.S. policymakers would need to determine the extent to which CMS or other organizations would be responsible for the implementation and management of an electronically readable system for Medicare. Some of the responsibilities that the French and German organizations address, such as certifying the software, are currently being addressed by another

agency within HHS.[60] Therefore, decisions would need to be made about the appropriate agencies or organizations that should be involved in developing and implementing such a system.

Concluding Observations

As consideration is given to whether to increase the functionality of the current Medicare beneficiary card, and whether to implement cards for providers, the planned use of the cards will guide the type of card technology that is needed. The planned use of the cards will also prompt additional discussions regarding card management processes and standards, including whether use would be mandatory, whether PINs or biometric factors would be used in addition to the cards, whether enrollment and card issuance processes would need to be updated, and what information would be stored on the card. We found that electronically readable cards would have a limited effect on program integrity, but could aid administrative processes. Ultimately, a decision about whether to implement an electronically readable card will rest upon a determination regarding the costs and benefits of electronically readable cards compared to the current paper card or other strategies and solutions. The success of any electronically readable card system will also depend on participation from health care providers, and therefore any planned use will need to take provider costs and potential challenges into consideration. Finally, as demonstrated by the experiences in France and Germany with smart cards, implementing and maintaining an electronically readable Medicare card system would likely require considerable time and effort.

Agency and Third-Party Comments and Our Evaluation

We provided a draft of this report to HHS for comment. HHS provided technical comments, which we incorporated as appropriate.

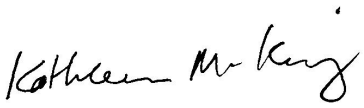
In addition, we obtained comments from officials from the Smart Card Alliance, an organization that represents the smart card industry. The officials emphasized the greater capability of smart cards to authenticate transactions and secure information on the cards than other electronically readable card options. Smart Card Alliance officials commented that the way in which CMS has indicated that it would implement electronically

[60]ONC establishes criteria that describe the minimum related performance standards and implementation specifications needed for EHR technology to be certified. ONC also oversees the certification of EHR technology.

readable cards in Medicare would diminish the cards' potential to limit fraud. Further, the officials commented that we underestimated the potential of electronically readable cards to further CMS's program integrity efforts, particularly CMS's ability to identify potential fraud through postpayment claims analysis. The officials said that CMS could have greater assurance in the legitimacy of claims associated with card use and that the agency could better focus its analysis on claims in which cards were not used. Finally, the officials commented that possible challenges applying NIST standards for using electronically readable cards in Medicare should not preclude card implementation because standards that better align with the needs of the program could be developed. We believe that our report accurately characterizes the potential effects of electronically readable cards on Medicare program integrity efforts, though we modified several statements to improve clarity. We also incorporated the Alliance's technical comments as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the Secretary of Health and Human Services, the Administrator of CMS, the National Coordinator for Health Information Technology, appropriate congressional committees, and other interested parties. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff members have any questions about this report, please contact me at (202) 512-7114 or kingk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.



Kathleen M. King
Director, Health Care

List of Requesters

The Honorable Ron Johnson
Chairman
The Honorable Tom Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Ron Wyden
Ranking Member
Committee on Finance
United States Senate

The Honorable Sander Levin
Ranking Member
Committee on Ways and Means
House of Representatives

The Honorable Kevin Brady
Chairman
Subcommittee on Health
Committee on Ways and Means
House of Representatives

The Honorable Peter Roskam
Chairman
Subcommittee on Oversight
Committee on Ways and Means
House of Representatives

The Honorable Mark Kirk
United States Senate

The Honorable Earl Blumenauer
House of Representatives

Appendix I: List of Organizations Interviewed

To examine the potential benefits and limitations associated with the use of electronically readable cards in Medicare and the steps CMS and Medicare providers would need to take to implement and use electronically readable cards, we interviewed officials from the agencies and organizations listed in table 2.

Table 2: Name and Description of Agencies and Organizations GAO Interviewed

U.S. organization	Description
AARP	Organization representing Medicare beneficiaries
Aetna	Health care insurer
America's Health Insurance Plans	Organization representing health care insurers
American Hospital Association	Organization representing health care providers
American Medical Association	Organization representing health care providers
AthenaHealth	Health care IT vendor
Centers for Medicare & Medicaid Services	Federal agency
Council for Affordable Quality Healthcare's Committee on Operating Rules for Information Exchange	Electronic health care transaction standards organization
Department of Veterans Affairs	Federal agency
Epic	Health care IT vendor
Gemalto	Electronically readable card vendor
General Services Administration	Federal agency
Health Level Seven International	Electronic health care transaction standards organization
Healthcare Billing and Management Association	Health care billing and management organization
Healthcare Information and Management Systems Society	Health care information technology organization
Kaiser Permanente	Health insurer
LifeMed ID	Electronically readable card vendor
Medical Group Management Association	Health care billing and management organization
Medical Identity Fraud Alliance	Anti-healthcare fraud organization
Medicare Zone Program Integrity Contractors	Centers for Medicare & Medicaid Services contractors that investigate potential Medicare fraud
Mount Sinai Hospital	Health care provider that has issued electronically readable cards to patients
National Health Care Anti-Fraud Association	Anti-healthcare fraud organization
National Institute of Standards and Technology	Federal agency
New York State Department of Health	State Medicaid program that has used electronically readable cards
North Carolina Department of Health and Human Services	State Medicaid program that has used electronically readable cards
Office of the National Coordinator for Health Information Technology	Federal agency
Resolute Health	Health care provider that has issued electronically readable cards to patients
Smart Card Alliance	Organization representing the electronically readable card industry
UnitedHealthcare	Health care insurer
Workgroup for Electronic Data Interchange	Health care information technology and standards development organization

French organization	Description
Agence des Systèmes d'Information Partagés de Santé	Organization managing an electronically readable card system.
Caisse Nationale de l'Assurance Maladie des Travailleurs Salariés	Organization representing health care insurers
Conseil National de l'Ordre des Médecins	Organization representing health care providers
Conseil National de l'Ordre des Pharmaciens	Organization representing health care providers
Cour des Comptes	Federal auditing agency
Fédération Nationale de la Mutualité Française	Organization representing health care insurers
Groupement d'Intérêt Économique SESAM-Vitale	Organization managing an electronically readable card system
Ministère des Affaires Sociales, de la Santé et des Droits des Femmes	Federal agency
German organization	**Description**
Bundesärztekammer	Organization representing health care providers
Bundesministerium für Gesundheit	Federal agency
Bundesrechnungshof	Federal auditing agency
Bundesvereinigung Deutscher Apothekerverbände	Organization representing health care providers
Deutsche Krankenhausgesellschaft e.V.	Organization representing health care providers
Gematik	Organization managing an electronically readable card system
GKV-Spitzenverband	Organization representing health care insurers
Kassenärztliche Bundesvereinigung	Organization representing health care providers

Source: GAO. | GAO-15-319

Appendix II: Information about Use of Electronically Readable Cards in France and Germany

Several European countries, including France and Germany, use electronically readable cards for health care purposes, such as transferring identity and insurance information electronically from the card to a health care provider's IT system. France and Germany have long-standing experience with the use of such cards. As part of our research on the potential use of electronically readable cards in Medicare, we visited France and Germany to learn about how they developed and used the cards. This appendix provides information on each country's health care system, and how electronically readable cards are used within that system.

France

French Health Care System

Health care coverage in France has been universal since 2000. All residents may receive publicly financed health care through noncompetitive health insurance funds (commonly referred to as statutory health insurance funds)—six entities whose membership is based on the occupation of the individual. Specifically, eligibility to receive statutory health insurance is granted either through employment (to salaried or self-employed working persons and their families) or as a benefit to persons (and their families) who have lost their jobs to students, and to retired persons. The state covers the health insurance costs of residents not eligible for statutory health insurance, such as unemployed persons.

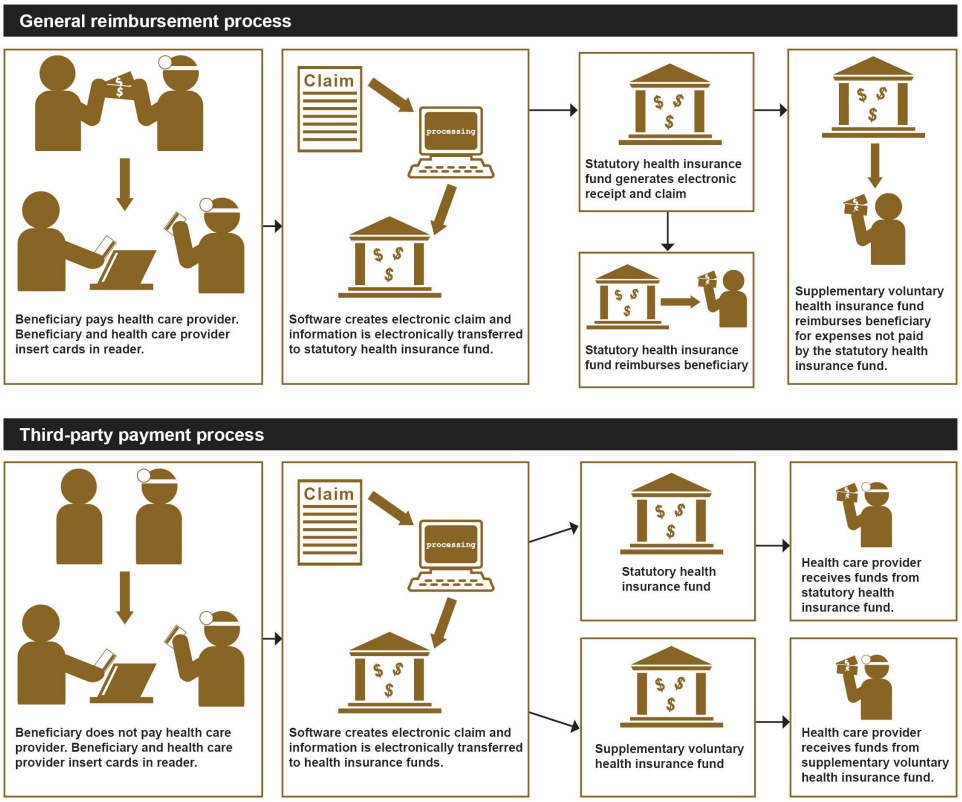
The French system of health insurance is composed of two tiers. The first tier provides basic coverage through the statutory health insurance funds, which cover about 75 percent of household medical expenses. The statutory health insurance coverage includes hospital care and treatment in public or private rehabilitation; outpatient care provided by general practitioners, specialists, dentists, and midwives; and prescription drugs. The second tier consists of complementary and supplementary voluntary health insurance coverage provided by mutual (not-for-profit) or private insurers that pay for services not covered by statutory health insurance.

Use of Electronically Readable Cards in France

France's health care system uses two electronically readable cards—a beneficiary card and a health care provider card—as part of its billing and reimbursement processes; both are smart cards.[1] Generally, beneficiaries make payment to the health care provider when services are delivered, and the health insurance funds reimburse the beneficiary. In certain circumstances, such as when services are provided by pharmacists and radiologists, third-party payment or reimbursement directly to the health care provider is used. When services are provided, the beneficiary and the health care provider both insert their cards into a two-card reader at the point of service. The software enables the health care provider to enter medical consultation information into the provider's IT system. That information is used to generate an electronic health claim form, which is sent to the statutory health insurance fund and the supplementary voluntary health insurance fund for payment to either the beneficiary or the health care provider. (See fig. 2.)

[1]The smart cards used in France are electronically readable cards with microprocessor chips that are capable of processing data.

Figure 2: Health Care Payment and Reimbursement Processes in France



Sources: GAO analysis of Fédération Nationale de la Mutualité Française information (data); GAO and Art Explosion (clipart). | GAO-15-319

Germany

German Health Care System

Health insurance has been mandatory for all citizens and permanent residents of Germany since 2009.[2] There are two primary sources of health insurance in Germany—the publicly financed health insurance (commonly referred to as the statutory health insurance system) and the

[2]Prior to 2009, certain populations could choose not to have insurance.

private health insurance system.[3] Under the statutory health insurance system, which covered about 86 percent of the population in 2013, health insurance is generally provided by competing, not-for-profit, nongovernmental health insurance funds (called "sickness funds"). As of January 2013, there were 134 sickness funds operating under the statutory health insurance system.

All employed citizens earning less than $4,874 per month ($70,489 per year) as of 2013 are covered by the statutory health insurance system, and they and their dependents are covered without charge.[4] Individuals whose gross wages exceed the threshold, civil servants, and those who are self-employed can choose to participate in statutory health insurance or purchase private health insurance, which covered about 11 percent of the population in 2013. Statutory health insurance coverage includes preventive services, inpatient and outpatient hospital care, physician services, prescription drugs and sick leave compensation. Private health insurance covers minor benefits not covered by statutory health insurance, access to better amenities, and some copayments (e.g., for dental care).

Use of Electronically Readable Cards in Germany

Germany first introduced a beneficiary, memory-only health insurance smart card in 1995.[5] German citizens who were members of a public, statutory health insurance fund were issued the memory-only card, which contained beneficiary insurance information. This card was used to electronically transfer the information stored on the card to health care providers' IT systems.

More recently, Germany initiated a project to modernize its health care system with the introduction of a secure network infrastructure. Part of

[3]Legal residents not covered by the statutory health insurance system (e.g., soldiers and police) are covered under special programs. Undocumented immigrants are covered by the social security system in case of acute illness and pain, as well as pregnancy and childbirth.

[4]There are some cost-sharing provisions for adults age 18 years and older, including copayments for inpatient and rehabilitation stays and some outpatient prescriptions. There is an annual cap on cost-sharing equal to 2 percent of the household income. Children under 18 years of age are exempt from cost-sharing.

[5]A memory-only smart card has a memory chip that can store data, but does not process data.

this project included updating the beneficiary smart card with a card that has the capability to store and process information. In 2011, Germany began issuing the updated smart card, which contains the same information as the memory-only card and is currently being used in the same way, which is to auto-populate health providers' IT systems. According to German officials, new applications will be added incrementally to the updated smart card, with the card eventually being used to access and update online beneficiary health insurance information and exchange beneficiary medical information. As of September 2014, officials told us that all applications will not be added until 2018.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Kathleen M. King, (202) 512-7114 or kingk@gao.gov.

Staff Acknowledgments

In addition to the contact named above, Lori Achman, Assistant Director; George Bogart; Michael Erhardt; Deitra Lee; Elizabeth T. Morrison; Vikki Porter; Maria Stattel; and Kate Tussey made key contributions to this report.

Appendix IV: Accessible Data

Data Tables for Figure 1: Comparison of the Functions and Technical Capabilities of Electronically Readable Cards for Potential Uses in Medicare

Authentication	Smart Card [Note A]	Magnetic Stripe	Bar Code
Resistance to counterfeiting or copying [Note B]	High	Low	Low
Ability to be used with public key infrastructure to ensure card authenticity [Note C]	Yes	No	No
Use with second authentication factor	Yes	Yes	Yes
On-card vertification of second authentication factor	Yes	No	No

Storing and exchanging medical information	Smart Card [Note A]	Magnetic Stripe	Bar Code
Storage capacity for medical information [Note D]	Medium	Low	Low
Ability to secure stored data [Note E]	High	Low	Low
Ability to limit access to information on the cards	Yes	No	No

Conveying identity and insurance information	Smart Card	Magnetic Stripe	Bar Code
Sufficient storage capacity to store identity and insurance information	Yes	Yes	Yes

Source: GAO analysis of industry, academic, and federal agency documents. GAO-15-319.

[a]The capabilities of smart cards depend on the particular chip used, and not all chips have all of these capabilities.

[b]This refers to the difficulty of counterfeiting or copying the electronically readable features or information on the cards. Physical security features, such as holograms or watermarks, can be used on all three types of cards to increase the difficulty of copying or counterfeiting the cards. For the purposes of this analysis, the high and low ratings are relative among the three types of cards and are based on capabilities that make the electronically readable features of the cards harder to recreate and can restrict access to information on the cards.

[c]Smart cards that are used in conjunction with public key infrastructure involve the use of public and private "keys." To authenticate the card using public key infrastructure, the card transmits information encrypted with a private key. The encrypted information can only be decrypted with a corresponding public key. Decrypting the information with the public key authenticates the identity of the card because the public key will only decrypt information that has been encrypted using the card's private key. The public key is made freely available to any entities that wish to be able to authenticate the card.

[d]The amount of storage capacity needed to store medical information on a card would depend on the content and file sizes of the information on the card. For this analysis, we defined low storage capacity as the ability to store a very limited amount of information; medium as the ability to store many pages worth of textual information, but not large data files; and high as the ability to store large data files. Although smart cards would be able to store significantly more medical information than cards with magnetic stripes and barcodes, it is unlikely that they would be able to store all of a beneficiary's medical records or larger file size medical records, such as medical images.

[e]For this analysis, the high and low ratings are relative among the three types of cards and are based on the presence of multiple electronically readable card capabilities that can restrict access to information on the cards.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Website: http://www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548