Smart Card Technology in U.S. Healthcare: Frequently Asked Questions

A Smart Card Alliance Healthcare Council Publication

Publication Date: September 2012

Publication Number: HCC-12002

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

About the Smart Card Alliance

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

TABLE OF CONTENTS

I. About Smart Cards

General Questions

1. What is a smart card?

A smart card is a small card or similar device with an embedded integrated circuit chip. Smart cards typically look like a credit card (Figure 1), although they can take different forms (Question 8 on p. 9). What makes the card smart is the embedded chip. The chip is a powerful minicomputer that can be programmed for different applications.

The chip enables a smart card to store and access data and applications securely and exchange data securely with readers and other systems. Smart card technology can provide high levels of security and privacy protection, making smart cards ideal for handling sensitive information such as identity and personal health information.

Figure 1. Example Smart Health Cards

2. How do smart cards work?

A smart card connects to a card reader either through direct physical contact or through a remote, contactless radio frequency (RF) interface. A typical contact smart card has a plastic card body, a chip embedded in the body, and a contact plate. The contact plate (usually gold-plated) is visible on the surface of the card (Figure 2).

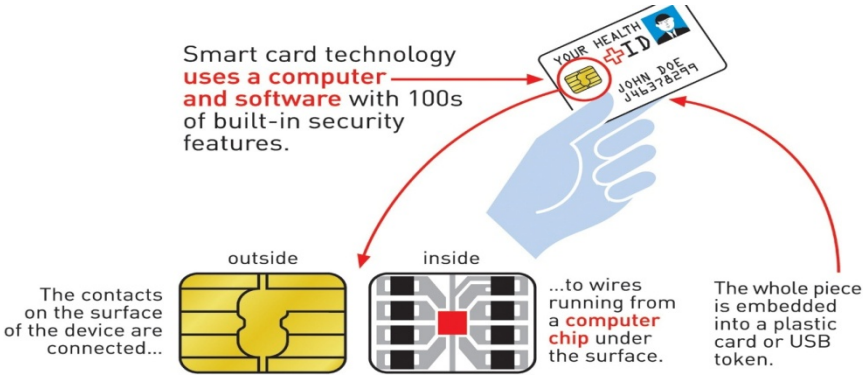

Figure provided courtesy of Gemalto.

Figure 2. Contact Smart Card Technology

To work, a contact smart card is inserted into a smart card reader, which touches the contact plate. Commands, data, and card status are transmitted over the physical contact points.

Contactless smart cards look like contact smart cards but without the contact plate. They communicate with the reader through a contactless RF interface. To work, contactless smart cards are held in close proximity to a reader and commands and data are transmitted without any physical contact.

3. How are smart cards used?

Smart cards are currently used for many applications worldwide, including:

- Identity applications: employee ID badges for physical access to buildings and secure computer and network access; citizen ID documents; electronic passports; driver's licenses; online authentication devices
- Healthcare applications: citizen and patient health ID cards; health provider ID cards; portable medical records cards
- Payment applications: contact and contactless credit and debit cards; transit payment cards
- Telecommunications applications: mobile phone subscriber identity modules; pay telephone payment cards

4. What kinds of healthcare information can smart cards store?

While some smart cards can securely link to cloud-based patient information systems, smart cards can also store a wide variety of information to support healthcare applications. Figure 3 illustrates examples of the types of healthcare information that may be stored on a smart healthcare card.

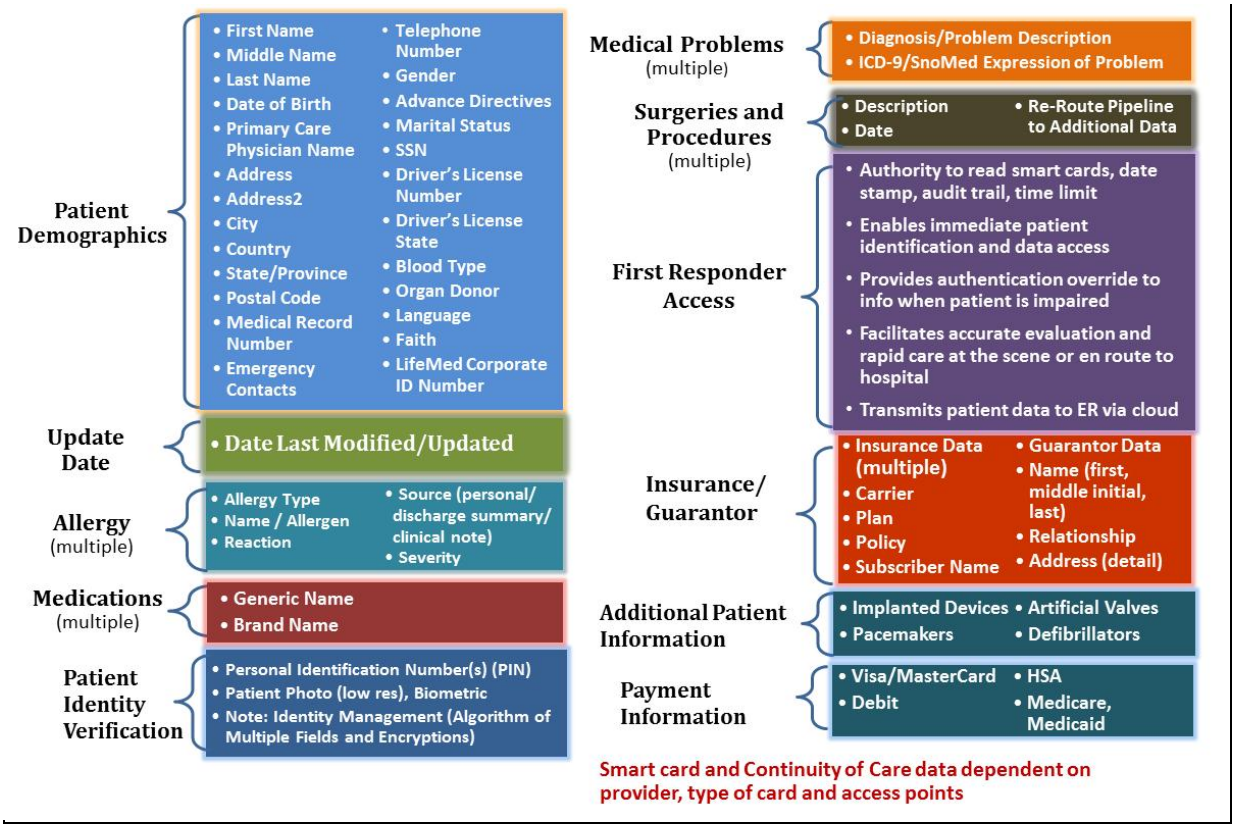

Figure 3. Examples of the Healthcare Information Smart Cards Can Store[1]

[1] Graphic provided courtesy of LifeMed ID, Inc.

5. What smart card security features can protect personal healthcare information?

Unauthorized access to sensitive personal healthcare information (PHI) is a critical concern, as more and more medical data is converted to digital format. Multiple security features enable smart cards to protect PHI—both information that resides on the card and information that resides on a remote server accessible over the internet.

The primary line of defense is the use of authentication methods that protect against unauthorized access to data stored on the card. Smart cards are commonly programmed to require a personal identification number (PIN). To protect the most sensitive PHI, smart cards can require multi-factor authentication, which is enabled by requiring a combination of three factors for access: something the person knows (e.g., a PIN), something the person has (e.g., the smart card itself), and something the person is (e.g., a biometric characteristic, such as a fingerprint). Smart cards can also be programmed to enforce user access rules allowing only authorized doctors, hospitals, and medical staff to access all or part of a patient's PHI.

Smart cards can protect stored data through the use of encryption and other cryptographic methods enabled by the card's microprocessor, such as key generation, secure key storage, hashing, and digital signatures.

Smart cards can also provide secure access to PHI contained in online records. Upon successful authentication, the patient's card is used to point directly to the individual patient's data on the server.

Smart cards support guidance from the U.S. Federal government initiatives that are aimed to protect online access to data, including:

- The National Strategy for Trusted Identities in Cyberspace, which identifies consumer access to online electronic health records as warranting the use of multi-factor authentication.
- Office of the National Coordinator for Health Information Technology guidance, which specifies that "HIE entities should establish strong identity proofing and authentication for user access to electronic health information" systems and recommends implementation of a Level 3 assurance level, as defined in NIST SP 800-63 version 1.0.2."[2]

Smart cards can validate their own authenticity using digital signatures. Digital signatures can confirm that the smart card was issued by a legitimate organization and that the data on the card has not been altered fraudulently since issuance. A smart card can also be programmed to authenticate the validity of a card reader or other device that accesses information from the card.

Smart cards are manufactured with security countermeasures that thwart cloning, counterfeiting, and tampering. Built-in security features include metal layers, sensors that detect thermal and UV light attacks, and software and hardware circuitry to thwart differential power analysis.

Depending upon the sensitivity of the data, the security features supported by smart cards can be used individually or in combination, creating a layered approach. The variety and efficacy of these security features make smart card technology extremely resistant to duplication, forgery, and tampering.

6. Do smart cards have advantages over magnetic stripe cards?[3]

Smart cards have significant advantages over magnetic stripe cards for healthcare applications.

---

[2] Department of Health & Human Services, Office of the National Coordinator for Health Information Technology, "Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program," Public Information Notice, Document Number ONC-HIE-PIN-003, March 22, 2012.

[3] The briefing, "Benefits of Smart Cards versus Magnetic Stripe Cards for Healthcare Applications," contains additional information on how smart cards compare with magnetic stripe cards and is available at http://www.smartcardalliance.org/pages/publications-benefits-of-smart-cards-versus-magnetic-stripe-cards-for-healthcare-applications.

First, smart cards are highly secure; they are used worldwide when the security and privacy of information are critical requirements. Both contact and contactless smart cards can support the high levels of security required to protect sensitive information and enable secure transactions.[4] Smart cards can protect healthcare information in a number of ways:

- Smart cards with embedded microcontrollers can encrypt and securely store a patient's personal health information.
- Smart cards can control who accesses the stored information.

  For example, the patient's personal health information can be protected so that only authorized doctors, hospitals, and medical staff can access all or portions of that information. The smart card can enforce rules for accessing a patient's medical information, even when used locally with a reader that doesn't connect to a central system.
- Smart cards can support multi-factor authentication.

  Patients and providers can use smart healthcare cards as a second factor when logging in to a computer system to access information. Smart cards can also support the use of PINs and biometric data (e.g., a fingerprint) for further access protection.
- Smart cards can support digital signatures, which are used to determine whether the card was issued by a valid organization and whether the data on the card has changed since issuance.
- Smart cards use secure chip technology and are designed and manufactured with features that help deter counterfeiting and thwart tampering.

Secure smart chip technology, encryption, and other cryptography measures make it extremely difficult for unauthorized users to access or use the information on a smart card or to create duplicate cards. These capabilities help protect patients from identity theft and healthcare institutions from medical fraud and can also help healthcare providers meet HIPAA privacy and security requirements.

Second, smart cards are flexible. Information can be added securely to a card after the card is issued. This flexibility means that patient healthcare information can be written to and updated on a smart card by authorized healthcare providers. Updated information is then available to both the patient and all authorized healthcare providers. For example:

- Patient prescriptions can be written to the card, providing up-to-date information when a patient is receiving medical care from multiple providers or in an emergency.
- Multiple patient identification or patient record identification numbers can be written to the card, facilitating record exchange and coordination of care among multiple healthcare providers.

Third, smart cards can store more information than magnetic stripe cards. Figure 4 compares the storage capacity of magnetic stripe and smart cards.

Fourth, smart card technology is incorporated into and can interoperate with mobile devices, such as Near Field Communication (NFC) enabled smart phones, laptops and tablet computers. This can enable secure transactions, such as financial transactions or secure access of personal health records by citizens or authorized health professionals using a myriad of portable devices.

In comparison, magnetic stripe cards are less secure with less functionality. Because data is read from and written to a magnetic stripe card easily, information can be stolen easily and a duplicate magnetic stripe card created. A thief can swipe a magnetic stripe card and collect all of the information from the card; the thief needs only a magnetic stripe reader (all readers have the ability to capture the information on a magnetic stripe card). The thief can then either use that information directly or create a duplicate magnetic stripe card. Moreover, magnetic stripe cards cannot be updated after issuance, providing no ability to securely update or store additional healthcare information.

Magnetic stripe cards have been established in the marketplace for over 30 years. However, industries and government organizations are becoming more aware of the limitations of magnetic stripe

[4] For additional information on how smart cards can protect sensitive information and enable secure transactions, see the Smart Card Alliance white paper, "What Makes a Smart Card Secure?," at http://www.smartcardalliance.org/pages/publications-smart-card-security.

technology. A case is being made for smart card technology to replace or augment magnetic stripe technology. If necessary, a magnetic stripe can be included on a smart patient healthcare card to support legacy applications.

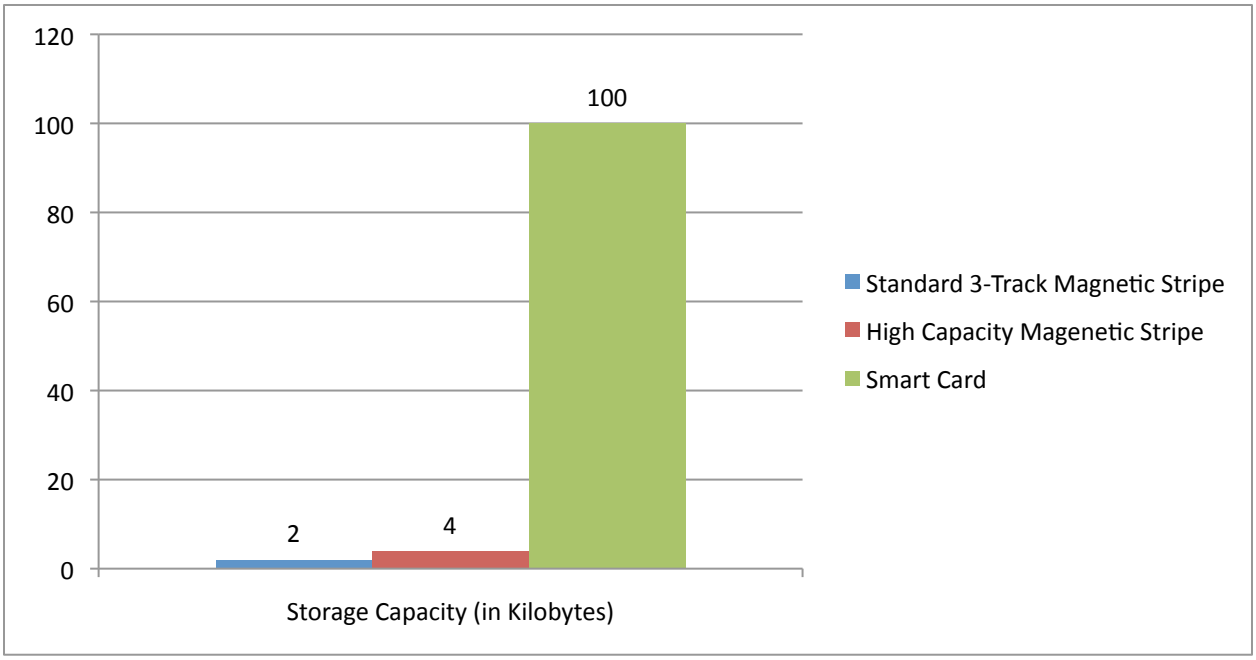

Figure 4. Storage Capacity of Magnetic Stripe Cards and Smart Cards

7. Is contactless smart card technology the same as RFID?

Contactless smart card technology is not the same as RFID. Discussions of RF-enabled applications can be confusing, and contactless smart card technology is often incorrectly referred to as RFID. Currently, a wide range of RF technologies are used for a variety of applications, each with different operational parameters, frequencies, read ranges, and security and privacy features. For example, the RFID technologies that are used to track inventory operate over long ranges (e.g., 25 ft.) and have minimal built-in support for security and privacy.

Contactless smart cards use RF technology but, by design, operate at short ranges (less than 4 in.) and are very secure. Contactless smart card technology is currently being used for secure identity applications worldwide.

8. Do all smart cards look the same?

Smart card technology conforms to international standards ISO/IEC 7816 and ISO/IEC 14443, which enable smart cards to be interoperable. Smart card technology is available in a wide variety of form factors (Figure 5), including plastic cards, key fobs, the subscriber identification modules (SIMs) used in GSM mobile phones, and USB-based tokens. Different applications may use different form factors depending on the application and end user requirements.

Figure 5. Examples of Smart Card Form Factors

9. Can smart cards store a patient's complete medical record?

Some smart health card implementations will provide secure access to cloud-based health information systems as a way of ensuring a patient's health information is protected and accurate.

However, smart cards are also available with a variety of features and memory capacity. A card equipped with 128 Kbytes of memory, for example, can store more than 120 pages of data. Large data files that cannot be stored on the card, such as lab reports or diagnostic images, can be stored on a central server and be accessed by the card. For example, emergency responders or an "outside" provider could use the card to access patients' health records stored on a server in the cloud. Since the card authenticates the patient's identity and carries additional medical and demographic data, it can be used as a key for authorized healthcare providers to unlock and access additional data.

10. Who can access the information on a smart card?

Smart cards are very secure. Access to the information on a card can be controlled and granted only to authorized personnel. A patient can control who accesses information, and access can be granted only with patient consent and given only to individuals identified by the patient or specified by policy. Access requirements can be defined; individuals may be given permission to access only specific information. For example, emergency personnel may need access only to details on allergies, prescriptions, or blood types. Access can also be controlled by PIN or biometric factor.

All access transactions can be recorded for audit purposes and reported.

The answers to Question 5 on p. 7 and Question 6 on p. 7 include additional information describing the security provided by smart cards.

11. What are the advantages of smart cards over a biometrics-only solution for identity authentication?[5]

Healthcare organizations considering different approaches for verifying patient and healthcare provider identity must look at the privacy, security, usability and performance implications of the different options. Smart healthcare cards – either alone or combined with biometrics – provide a privacy-sensitive, secure solution, and also offer additional features and functions that can provide significant benefits to healthcare providers when compared to a biometrics-only solution.

Biometrics-only solutions are not ideal for patient health ID cards. A smart healthcare card with a photo provides a solution that patients are familiar with and will readily accept. In addition, the smart healthcare card promotes the healthcare organization brand, can support a wide variety of applications that add value, and can be interoperable and usable among disparate groups.

[5] See the white paper, "Smart Cards and Biometrics in Healthcare Identity Applications," for additional information on the key considerations for selecting biometric and smart card technology for identity verification and a detailed comparison of biometrics-only, smart card and combined biometrics/smart card solutions. The white paper is available at http://www.smartcardalliance.org/pages/publications-smart-cards-and-biometrics-in-healthcare-identity-applications.

Either a smart provider ID card or a smart provider ID card with a biometric can provide healthcare organizations with the features needed to authenticate provider identities and offer better performance than a biometrics-only solution. Providers need an identity authentication solution that can be used at multiple facilities and in emergency situations. Smart healthcare cards are built on standards, can be interoperable across multiple locations, and can be used with portable readers in emergency response situations. For multi-factor authentication, a smart healthcare card with a PIN can be significantly more cost-effective for a healthcare organization than a biometric solution.

Combining smart cards and biometrics can provide a full-feature solution for healthcare provider identity authentication. By storing the biometric and performing the biometric match on the smart healthcare card, the privacy and security of biometric authentication are enhanced and system performance is improved, with local, offline identity authentication.

Only identity verification solutions based on smart card technology can provide identity assurance and authentication while increasing privacy and security. Smart cards also bring operational efficiencies to the healthcare system that reduce costs, reduce fraud, and increase patient satisfaction. As electronic health records (EHRs) and personal health records (PHRs) move to the mainstream, smart health ID cards can be used as a two-factor authentication mechanism into a provider or insurer web portal. Smart healthcare cards protect patient privacy and security when accessing online records and support the National Strategy for Trusted Identities in Cyberspace (NSTIC), which identifies consumer access to online electronic health records as warranting two-factor authentication.

Smart card technology is used globally for secure identity, access and payment applications. As a standards-based technology, smart card solutions for patient and provider identity management are deployed around the world and are available from numerous vendors. Smart card technology provides a strong foundation for healthcare ID cards, enabling improvement in healthcare processes and in patient and provider identity verification, while securing information and protecting privacy.

II. Smart Cards and the Healthcare Ecosystem

General Questions

1. Who benefits from smart cards?

Three entities can benefit from the use of smart cards as healthcare cards:

- Providers
- Patients
- Payers

How Providers Benefit

Healthcare providers are the professionals or institutions that provide healthcare services to individuals, families, or communities. Individuals who provide these services include practitioners (physicians, nurses, dentists, pharmacists) and other healthcare professionals. First responders, such as emergency medical services, are also included in this category. Institutions considered to be providers include privately and publically operated hospitals, clinics, and primary and urgent care centers. As the healthcare system evolves, new types of providers are emerging, such as accountable care organizations, which bring physicians and hospitals together in a provider network that shares responsibility for a patient's care.

Providers can realize the following benefits from implementing smart cards:

- Cost minimization
- Positive patient identification
- Administrative efficiency
- Regulatory compliance
- Enhanced patient satisfaction
- Better patient outcomes
- New revenue streams
- Competitive differentiation

Cost minimization. The use of a smart card can minimize costs by reducing identity errors during the registration process, eliminating the denial of claims due to incomplete demographic or insurance information, and automating and streamlining the registration process, allowing personnel responsible for registration to be more efficient and focus on higher value tasks.

Positive patient identification. When identification is authenticated by a smart card, the link between the card and the cardholder is validated, thereby mitigating the risks arising from mistaken or fraudulent claims of identity. Mistaken identity can lead to unnecessary or potentially harmful medical procedures and an inaccurate medical history record that can jeopardize future care for the patient to whom the record belongs.

Administrative efficiency. Smart cards can contribute to administrative efficiency by eliminating the repetitive task of manually creating and checking paper registration forms, freeing administrative personnel to focus on higher value tasks. Getting registration information right the first time eliminates the cost of using staff to resolve issues that delay the claims process.

Smart cards issued to healthcare providers as employee IDs can enable convenient, secure multi-factor authentication capabilities to access health information systems in facilities (e.g., hospitals, clinics), via authorized portable devices or to provide VPN access.

Regulatory compliance. Smart cards can also facilitate compliance with government regulations and industry rules. The use of a smart card can help covered entities and American Recovery and Reinvestment Act (ARRA)-stipulated entities comply with both the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the security and privacy mandates under ARRA.

Enhanced patient satisfaction and outcomes. Patient satisfaction should increase when the patient carries a smart healthcare card. Because smart cards expedite the registration process and make timely and accurate information about the patient's health status available to the provider, they minimize patient inconvenience and maximize the quality of the patient's interaction with the provider. By enabling positive patient identification and delivering relevant and accurate health data to the provider, smart cards play an important role in ensuring that the right treatment is given to the right individual on a timely basis.

New revenue streams. The convenience and quality of service to which smart cards contribute can build patient loyalty, resulting in return visits and increased use of provider services and thereby encourage new revenue streams. And because smart cards can support payment functions (debit and credit), they can be issued to facilitate incremental purchases of goods and services.

Competitive differentiation. Smart cards can deliver real and perceived benefits that can distinguish an issuer from that issuer's peers. The enhanced quality of service associated with smart cards can increase patient retention rates and attract new patients who are interested in a better healthcare experience. A sophisticated healthcare credential based on a smart card reflects well on the institution that issues it and gives the cardholder a sense of being a valued member of a prestigious organization. Furthermore, smart cards can interoperate with a wide range of mobile devices, providing healthcare providers with a secure way to access their patients' health information via a myriad of platforms and mobile devices. This supports the "bring your own device" (BYOD) strategies that many institutions are looking to adopt while giving providers innovative technologies to make them more productive.[6]

How Patients Benefit

Patients are the recipients of medical care, and with the advent of patient-centered care, these individuals play an increasingly important role in how healthcare is delivered. Patients derive the following benefits from using smart cards:

- Empowerment
- Convenience
- Better medical outcomes

Smart healthcare cards can give patients personal ownership and control over their medical records, enabling them to receive well-informed treatment more quickly. Smart cards can expedite the registration process, resulting in care delivery that is distinguished by greater speed and efficacy.

Because smart cards deliver a positive identification along with the patient's medical information, they can support expeditious delivery of the most appropriate treatment. In emergencies, a smart healthcare card can enable immediate access to potentially lifesaving information. For example, emergency responders can read information about a cardholder's medication allergies from a smart card and treat the person with appropriate medication.

Smart healthcare cards can also provide patients with secure access to their health information via emerging online patient portals and mobile applications, which are becoming increasingly important as healthcare treatment efforts shift to non-traditional settings such as the home.

[6] Additional information on the use of smart card technology and mobile devices for identity authentication can be found in the Smart Card Alliance white paper, "Mobile Devices and Identity Applications," available at http://www.smartcardalliance.org/pages/publications-mobile-devices-and-identity-applications.

How Payers Benefit

Payers are the parties outside of the physician-patient relationship that finance patient care. Included in this category are government agencies, such as the Centers for Medicare and,Medicaid Services (CMS) and the Veterans Administration, and private insurance companies. Private insurance companies can be divided into for-profit businesses, such as Aetna, CIGNA, and Oxford, and not-for-profit businesses. Certain insurance companies fuse public and private insurance, supplementing government insurance (such as Medicare) with private insurance coverage. Included as payers are the health maintenance organizations (HMOs) that offer both basic Medicare coverage and private insurance paid for by patient-paid premiums and flexible spending accounts (FSAs).

Smart cards can help payers save money. They can fit into a payer's enterprise IT automation strategies to improve administrative savings by streamlining business processes and providing better patient care. In addition, authentication of the cardholder as the insured reduces medical fraud by eliminating card swapping, tampering, and cloning. Smart cards can support verification of benefits eligibility at the point of service, ensuring that treatment is restricted to covered services and prescriptions. The availability of a patient's up-to-date healthcare record at the point of service reduces the incidence of duplicate tests and procedures that are typically a significant cause of wasteful spending.

Smart healthcare cards can also address provider fraud by providing strong authentication of the healthcare provider identity when submitting a claim and by linking treatments with verified patient encounters.

2. How many smart cards are currently deployed in the healthcare market?

Smart cards are not a new technology. Over 5 billion smart cards are issued annually worldwide; over 140 million have been distributed in healthcare alone. (See Section IV, question 10, for examples of smart healthcare card implementations.)

3. Have any stakeholders in the healthcare ecosystem deployed smart cards?

Healthcare providers (hospitals, physicians, and clinics) are currently using smart cards. The healthcare market has accepted the technology and is implementing patient identity solutions using smart cards in combination with identity software solutions. See Section IV, question 3, for examples of smart healthcare card implementations.

Implementation Considerations

4. What are the major barriers to smart healthcare card implementation?

The major obstacles to smart healthcare card deployment are overburdened IT departments and budgetary constraints. The urgency of deploying priority projects, such as electronic medical records, has completely absorbed most IT resources. Major government health insurance programs like Medicare and Medicaid are being cut or are facing significant reductions.

In actuality, smart healthcare card implementation may not require significant IT resources. Today's technology provides an opportunity for healthcare providers to interface smart card software with their current patient admissions software. Integration can be accomplished without involving teams of provider IT personnel; more important, integration does not disrupt the provider's current workflow at patient registration or admissions, since the current registration systems can be used. In fact, the registration process may become easier, since use of the smart card can assist in automating registration.

Providers implementing smart healthcare cards can counter budget constraints by pointing to potential savings. Cost savings can be calculated using time and cost data for current registration procedures. Providers can measure savings in areas such as data entry time, registration time, key stroke entry errors, billing errors and delays, and duplicate and overlaid record errors and repairs. The savings

realized annually can pay for a typical smart card deployment, as illustrated by a case study at Memorial Hospital (Conway, N.H.), which verified a return on investment (ROI) within 8 months (Question 14 on p. 18).[7]

The Medical Group Management Association (MGMA) has taken a leadership role in promoting the use of readable patient healthcare cards compliant with the standards promulgated by the Workgroup for Electronic Data Interchange. The MGMA estimates that the total cost savings attributable to implementation of an electronically readable patient healthcare card are over $2.2 billion per year in the United States.[8] This number was calculated using conservative estimates of the amount of time and money attributable to resubmitting claims, making copies, and manually entering patient data. A healthcare provider can use the same matrix to determine annual cost savings for a facility, using either the conservative MGMA estimates or entering the provider's own numbers, if available.

Figure 6 illustrates how to calculate the estimated annual cost savings for a provider using automated smart card registration technology. The example shown is a 160-bed hospital that registers 590 visits per day, provides 14,000 emergency room visits and 200,000 outpatient visits, and admits 1,800 patients per year.

5. How much time is required to roll smart healthcare cards out to cardholders?

The amount of time required to roll out a smart healthcare card depends on the scope and complexity of the solution that is being implemented. Smart card technology is available that can interface to a provider's system in a matter of days, using healthcare messaging standard (HL7) and hosted cloud solutions. Smart cards require minimal amounts of hardware, and the hardware is "plug and play," so impact on registration workflow is typically minimal. Other considerations are the scope of the solution and the number of system interfaces involved.

Providers typically roll a system out to either a segment of their patient base or every patient who enters a facility. Timing depends on what the specific solution the provider wants to implement. For example, an encrypted, branded card with a photo, name, and required demographic and medical information can be provided to each patient at registration. Or cards can be mass distributed to a target patient base; as patients return to the facility with their cards, provider personnel can verify their identity, take pictures of the patients, and activate the cards.

6. Is a unique patient ID needed to use smart healthcare cards?

Ensuring that a person's medical record information is complete, safe, and accurate is a challenge, given the involvement of multiple pharmacies, physician's offices, hospitals, urgent care centers and other medical providers. The task is complicated by the fact that individuals change employers, insurance carriers, insurance plans within a carrier, and names.

Some countries have chosen to address this complexity by issuing national health ID cards, with each citizen having a unique identifier. However, smart cards can support healthcare applications with or without a unique patient identifier. Smart cards can serve as a secure way to correlate multiple identifiers across different systems and organizations, linking them all on the card.

7. Can smart cards integrate with current healthcare applications and workflow?

Smart cards allow for electronic interfacing with healthcare identity software solutions. Healthcare identity software integrates with current healthcare applications, including admissions discharge transfer applications, electronic medical records, electronic healthcare records, and health information exchange applications.

[7] Lawrence Carbonaro, "Memorial Hospital: A Case Study," 2009, http://www.lifemedid.com.
[8] MGMA Project SwipeIt,,"Model Assumptions and Raw Input," 2009, http://www.mgma.com/swipeitwaste.

Annual Savings Calculator

** "**Change ONLY Yellow Cells"** to match your current statistics. Otherwise you may use **MGMA's*** conservative National Averages** **Follow Color Matched Cells**

Annual Time Savings Calculator	Enter Number				
Enter average number of patients registered per day	590				
	Est. Percent	Number/Factor			
Enter percentage of patients whose information needs to be updated?	8%	47.2			
Patient Processing Time	**Change Data Accordingly**	**Time (minutes)**	**Hours Per Day**	**Conservative Hourly Wage**	**Yearly Savings**
Average time spent verifing identity of the patient using existing process?	3	1770	29.5		
Average time to look up patient record?	3	141.6	2.36		
Average time to make copies and file in the correrct spot and give patient copy?	3	3	29.5		
Average time to update record on patient file and billing system?	15	1911.6	31.86		
Billing - A/R					
Average percent of denied claims per day?	6%	35.4			
Time to re-verify and re-submit claims denied because of incorrect information on conventional insurance cards? **Enter average number of minutes per claim.**	15	531	8.85		
Admission Data Entry Errors					
Admissions error rate due to data entry? **Enter average % per day**	6%	35.4			
Time for manual intervention to correct admission errors? **Enter average number of minutes per record to correct errors**	20	708	11.8		
System Down Time Registration					
Hours per week your system is typically down?	0				
			Hours Per Day Saved	**113.87**	
			Reoccurring Annual Hours Saved:	**29,606**	**$ 22.00**	**$ 651,336**

Annual Cost Savings Calculator					
Annual cost savings by reducing duplicate medical records	**Change Accordingly**	**Actual Numbers**			
Enter the number of medical records in your systems database	75,000				
Enter Percentage of duplicate or split records **(Nat'l Average of 5%-15%)**	7.0%	5,250			
Cost to detect and correct each record **(National Average of $20)**	$35	$183,750			
Average Annual **cost of paper** to register a patient?	$5,000				
			Reoccurring Annual Administrative Cost Savings:	**$188,750**	
			Cost Savings and Employee Time Saved - applied to reoccurring "Yearly ROI" Dollars		**$ 840,086**

Note: This model does not include other benefits of electronic registration.

Figure 6. Annual Savings Calculator Example[9]

[9] This model was provided courtesy of LifeMed ID.

8. Can smart healthcare cards help prevent identity theft?

A recent study estimates that nearly 1.5 million Americans are victims of medical identity theft.[10] The average cost to resolve a single case of medical identity theft is $20,663. The same study found that in 63 percent of the cases, the victim's name was used to obtain medical treatment or service, and in 43 percent, the victim's name was used to obtain government benefits, such as Medicare and Medicaid. The Secure ID Coalition estimates that the use of smart cards could eliminate $30 billion a year in Medicare fraud alone.[11]

Information on smart cards can be encrypted and smart cards can carry encoded identification verifiers, preventing electronic identify theft. In addition, smart cards can carry a photo (on the card, in the chip, or both) for physical identity verification. These measures, coupled with other authentication mechanisms such as the requirement for a PIN or biometric data (a fingerprint or iris scan, for example), can prevent would-be thieves from claiming and using a card. More important, smart healthcare cards can carry a universal identifier and be linked to a patient's medical record number or master patient index number. The card's use can then be tracked or date-stamped to log and verify activity.

Operational Considerations

9. How are cardholders prevented from "sharing" a card?

Unlike insurance cards and government beneficiary cards (such as Medicare and Medicaid cards), smart cards can carry encoded authentication verifiers, including a photograph, PIN, and biometric data. When a smart healthcare card is issued, the patient's identity should be verified. When the patient presents the card, these authentication verifiers can be used to verify the patient's identity at the point of service.

In addition, the card can carry a universal identifier that identifies the patient's medical record or master patient index number. It would be difficult for a different person to use the card, even if that person resembled the patient, because the card can retrieve the correct cardholder's medical record automatically at registration.

10. How is information on a card updated when cardholder information changes?

When a patient uses a smart healthcare card, whether at a registration desk or at a kiosk, the patient should be prompted for any information changes, such as change of address or insurance. After any new information is recorded in the provider's system, the updates can automatically be stored on the card.

Healthcare identity software is available that can correlate patient visits across different locations. That is, if a patient updates information at one location and then uses the card at another location, the card can electronically alert staff that information has been changed, allowing them to verify with the patient that the changes are correct. In addition, the new data on the card can update the information on the provider's system with a click of the mouse. This approach both automates manual data entry and closes the information gap between different providers using software systems that do not communicate. Such information gaps can be costly to providers and inconvenient for patients. Perhaps more important, the most current information can be available to a healthcare provider when a patient is unresponsive or cannot communicate.

11. Can card data be accessed in emergencies?

Solutions can allow first responders to access the demographic, medical, and insurance information on a smart card during an emergency. The critical medical information on the card can be read by emergency

[10] Ponemon Institute© Research Report, "Second Annual Survey on Medical Identity Theft," March 2011, http://www.protectmyid.com/images/education_center/pdf/050TypesofFraud/1_types%20of%20fraud_medical%20study.PDF.

[11] Secure ID Coalition, http://upgradethecard.com/

personnel using current communication hardware, such as a tablet computer with a card reader or a mobile phone. In the event of a disaster, the information on the card can be accessed without requiring an Internet connection or electricity. (These capabilities are why the American Medical Association endorses smart cards as the solution for populations in areas at risk of natural disaster.)

12. Who maintains the demographic data on smart cards?

The cardholder is responsible for ensuring that demographic data is current. When a cardholder enters a provider location and the card is read for that visit or for registration, the card can be updated with the most current data. Current card technology can interface the card with the provider's system to mirror the data on the card. Any information that changes at registration or after a medical visit can automatically be updated on the card by inserting the card into a reader at discharge.

Business Considerations

13. Which stakeholders typically pay for or issue smart cards?

There is no requirement that a particular stakeholder purchase the card. Any authorized organization can purchase and issue the card.

14. Can the return on investment for smart cards in healthcare be demonstrated?

A case study demonstrating both the use of smart healthcare cards and the return on investment (ROI) was conducted at Memorial Hospital, North Conway, N.H. in 2009.[12] The hospital is a 35-bed facility with 100,000 annual patient visits. The case study was conducted over an 8-month period, with the following results:

- Annual administrative savings of $300,000 (not including marketing advantages).
- Increase in Press Ganey patient satisfaction scores by 10 percent in the first 60 days. Scores are now in the top 5 percent for all providers nationwide.
- Decrease in billing errors from 6.8 percent to less than1 percent.
- Decrease in duplication of medical records from 7 percent to less than 1 percent, resulting in annual savings of $574,000 (scrubbing records), with unreported cost savings that include the costs of billing losses, medical procedure losses, and medical errors.
- Decrease in payment times for receivables from 55+ days to less than 42 days.
- Decrease in average admission time from 22 min. to less than 3 min., allowing Memorial to redirect staff to other tasks.
- Elimination of clipboards and paper at registration. A cover sheet given to the patient at registration is no longer required, saving 156 cases of paper and toner, and eliminating the requirements for storage and shredding of cover sheets.
- Reduction in full-time staff requirements from 22 to 15 (annual savings equates to $226,000).
- Decrease in admissions error rates from 6 percent to less than 1 percent (average 1,500 registrations a week).

15. Can smart cards contribute to effective health information exchange without national positive patient identification?

A smart healthcare card can carry a single unique identifier that authenticates the cardholder and connects all medical record numbers to one card identity. However, the card alone will not meet the requirements for nationwide positive patient identification. What is needed is a cloud-based unified

[12] Lawrence Carbonaro, *op cit*.

identifier that can connect to disparate identity software solutions and an open-source, universally adopted card-acceptance solution. The current smart card identity software solution providers provide the foundation required to attain these goals.

16. What happens if cardholders forget their cards?

If a card is forgotten, the registration process can proceed as if the patient forgot an insurance card. If an identity solution is in place at the provider's location, a photo of the person is displayed on all registration screens to help authenticate the patient's identity. If a card is lost, a new card is issued that can automatically connect to any current medical record numbers that were connected to the old card, and the old card is permanently terminated, rendering it useless.

Regulatory Issues

17. Can smart healthcare cards facilitate HIPAA compliance?

Smart healthcare cards offer an effective tool for facilitating compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. One of the key provisions of the HIPAA Privacy Rule is to assure that an individual's health information is properly protected and that individuals can control how their health information is accessed and used.

The HIPAA Privacy Rule applies to specific entities such as healthcare providers (doctors, dentists, pharmacies, nursing homes), health plans (HMOs, health insurance companies, company health plans), and health clearinghouses. Providing both employees of covered entities and patients with smart cards can ensure that health information is accessed only by those with the appropriate credentials.

Breaches of protected health information occur when data is kept on unsecured, unencrypted devices such as CDs and USB flash drives or when employees at covered entities access medical records without authorization.[13] Smart card credentials can minimize or eliminate such breaches by allowing only authorized personnel to access patients' medical records.

With the issuance of smart healthcare cards for patients, personal medical information on file with multiple institutions and care providers can be linked, securely and accurately. Patients can have better control of their personal health information, a key privacy principle. Accurate patient identification, a critical issue in healthcare today, supports the safety and confidentiality of protected health information.

18. Can smart healthcare cards facilitate American Recovery and Reinvestment Act compliance?

The American Recovery and Reinvestment Act of 2009 (ARRA) creates enhanced privacy standards. Smart healthcare cards address a key ARRA concern regarding access to health information. ARRA establishes a committee to examine methods that facilitate secure access by an individual to that individual's protected health information, as well as methods, guidelines, and safeguards to facilitate secure access by caregivers, family members, or a guardian.

The HIPAA Privacy Rule protects all individually identifiable health information held or transmitted by a covered entity. ARRA expands those protections beyond the HIPAA rule to include additional entities, such as vendors of personal health records. Smart cards can help covered entities and ARRA-stipulated entities comply with both the HIPAA Privacy Rule and the ARRA security and privacy mandates.

[13] "New Ponemon Institute Study Finds Data Breaches Cost Hospitals $6 Billion; Patient Privacy in Jeopardy," FierceHealthcare, November 9, 2010, http://www.fiercehealthcare.com/press-releases/new-ponemon-institute-study-finds-data-breaches-cost-hospitals-6-billion-pa.

19. What is "meaningful use" and can smart healthcare cards facilitate compliance?

Meaningful use of health information technology is an umbrella term for rules and regulations with which hospitals and physicians must comply to qualify for federal incentive funding under the American Recovery and Reinvestment Act of 2009 (ARRA).[14] ARRA authorizes the Centers for Medicare and Medicaid Services (CMS) to provide reimbursement incentives for eligible professionals and hospitals that meet meaningful use criteria on the way to becoming "meaningful users" of certified electronic health record (EHR) technology. Meaningful use includes using EHR technology for functions that both demonstrate and improve quality of care, such as e-prescribing, electronic exchange of health information, and submission of quality measures to CMS.

Meaningful use sets healthcare goals, rather than goals for information technology. The overall goals are to use EHR technology for the following:

1. Improve quality, safety, and efficiency of patient care
2. Engage patients and families
3. Improve care coordination
4. Ensure adequate privacy and security for personal health information
5. Improve population and public health

Implementation of meaningful use is occurring in multiple stages.

Stage 1 implementation requirements and measures are documented in the Department of Health and Human Services Final Rule of July 28, 2010.

The Department of Health and Human Services' Office of the National Coordinator (ONC) states that EHRs provide the following benefits for providers and their patients:[15]

- Complete and accurate health information.
- Better access to health information.

  EHRs facilitate access to the information that providers need to diagnose health problems earlier and improve the health outcomes of their patients. EHRs also allow information to be shared more easily among doctors' offices and hospitals and across healthcare systems, leading to better coordination of care.
- Patient empowerment.

  EHRs empower patients to take a more active role in their health and in the health of their families. Patients can receive electronic copies of their medical records and share their health information securely over the internet with their families.

The Stage 2[16] rules document includes:

1. Minor changes to Stage 1 criteria and measures
2. Additional requirements and measures for achieving Stage 2

[14] Meaningful use is a broad topic. For more information, follow the links to "EHR Incentives" at The Centers for Medicare and Medicaid Services Web site: https://www.cms.gov. Dr. John Hamalka's blog (http://geekdoctor.blogspot.com/2011/01/bookmarked-final-rules.html) contains bookmarked versions of the CMS final rules. Additional resources are the Healthcare Information and Management Society (HIMMS), "Meaningful Use One Source," http://www.himss.org/ASP/topics_meaningfuluse.asp, and "Ten Ways in Which LifeMed™ Smart Card Solutions Meet HITECH Act Initiatives: Helping Healthcare Providers and Organizations Improve Care Delivery, Reduce Costs, and Achieve Meaningful Use," http://www.midwestcard.com/attachments/category/56/10%20Ways%20in%20Which%20LifeMed%20ID%20Smart%20Card%20Solutions%20Help%20Healthcare%20Pro-viders.pdf.

[15] http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__meaningful_use_announcement/2996

[16] The final rule for Stage Two criteria for eligible professionals, hospitals, and critical access hospitals to qualify for Medicare and/or Medicaid EHR incentive payments is available at http://www.ofr.gov/OFRUpload/OFRData/2012-21050_PI.pdf.

3. Additional clinical quality measures
4. Additional reporting requirements and mechanisms

Implementation of meaningful use and incentive payment opportunities extends until at least 2020, with incentives decreasing over time to encourage early adoption of EHR technology.

Smart cards can make critical information readily available to healthcare providers and facilities, which positively affects the quality, accuracy, and cost of care. Current technology supports smart card solutions that can integrate with current provider systems using the cloud and HL7 messaging. Health information can be exchanged among providers and across systems, making key health information mobile and facilitating coordination of care. This same technology also allows healthcare information to be transformed into a standardized electronic format that can be accessed by patients and their families through secure patient portals.

Smart card and patient identity technologies can provide a modular EHR solution and meet Health Information Technology for Economic and Clinical Health (HITECH) and meaningful use requirements in eight areas:

1. Streamline patient registration and discharge
2. Fulfill government requirements for confirming identity verification
3. Increase patient privacy and security
4. Prevent record duplication
5. Provide consistent branding across an organization and beyond
6. Serve as a real-time, portable mini-EHR
7. Provide first responders with potentially life-saving information
8. Satisfy HIPAA compliance requirements

Streamline registration and discharge. Use of a smart healthcare card for registration or admission allows healthcare organizations to decrease patient wait times, improve the quality of care, and heighten efficiency by confirming a patient's identity, registering or checking the patient in, and verifying insurance instantly. Because the process does not rely on human data entry or transcription, errors can be virtually eliminated. Use of a smart healthcare card at discharge allows the system to recognize a patient's identity, match it to the visit, update the card with demographic and medical information, update a patient data portal with required discharge information (e.g., follow up appointments, medication information, education, instructions, activity requirements, dietary care), and trigger transmission of any required educational materials to the patient's e-mail address.

Meet government identity verification requirements. Smart card technology is currently used for the Department of Defense Common Access Card (CAC), the Federal Information Processing Standard (FIPS) 201 Personal Identity Verification (PIV) card (issued to all Federal employees and subcontractors), the Transportation Worker Identification Credential (TWIC), and the U.S. electronic passport. Using standards such as FIPS 201, smart cards can provide single sign-on solutions to EHRs for government-employed medical personnel, such as physicians and nurses.

Increase patient privacy and security. Smart card solutions can meet or exceed all mandates and requirements for patient privacy, safety, records, system security, and confidentiality. All smart card data can be encrypted, and all data transmitted can comply with applicable standards (e.g., HL7, SnoMed, and ISO/IEC). Medicare and Medicaid data and statistics can be maintained per federal requirements.[17] Smart cards integrated with an identity software solution can also support automated time-based reporting and review of patient data, protecting healthcare information with encryption algorithms that allow access only by authorized readers. Smart cards can support multi-factor authentication, which

[17] https://www.cms.gov/informationsecurity/downloads/ssl.pdf. CMS has defined 11 information types processed by CMS information systems. For each information type, CMS used FIPS 199 to determine an associated security category. CMS also used OMB M-04-04 to determine each information type's e-Authentication assurance level.

satisfies requirements such as those for e-prescribing, and can provide strong authentication, digital signatures, and security through encryption.

Prevent record duplication. Smart cards can significantly decrease the incidence of duplicate records and the associated expense. Linking a patient to that patient's health records seems a simple process, but human error, such as transcription of the wrong medical record number, can retrieve an incorrect record or cause creation of a duplicate record because the correct record has not been located. Using authenticated identifiers on a card can match a patient to that patient's individual medical record, improving administrative functions such as billing and registration and enhancing continuity of care.

Provide consistent branding. While smart cards can provide a single tool for patient identity management, they also provide healthcare organizations and affiliations with the opportunity to build stronger community alliances between healthcare organizations, integrated delivery networks, hospital systems, provider networks, and auxiliary services. Coupled with identity software, smart cards can replace multiple cards (e.g., insurance IDs, allergy cards, registration cards) that a patient or consumer would otherwise have to carry to be known throughout the organization. In addition, there are smart card solutions that make the patient's healthcare provider of record immediately known and recognized to other members of the healthcare community, such as pharmacies, durable equipment providers, and others.

Serve as a real-time EHR. Smart cards can contain encrypted patient demographic information, such as name, date of birth, height, weight, and body mass index (BMI), as well as other key information. In addition, a smart card can store key health data components such as current medications, allergies, immunizations, a conditions or problem list, smoking status, surgeries, and hospitalizations. Smart cards can also be configured to store patient information such as implanted devices, artificial valves, defibrillators, advance directives, and organ donation status. Unlike standard EHRs, a smart card is mobile and goes with the patient.

Provide first responders with critical information. In an emergency, smart cards can enable first responders using a simple portable reader to identify a patient immediately and access the patient's medical record, regardless of whether the patient is conscious, is emotionally or physically able to convey the entire medical picture accurately, or has language barriers that impede effective communication.

Satisfy HIPAA compliance requirements. Smart healthcare cards offer entities covered under HIPAA an effective tool to facilitate compliance with the HIPAA Privacy Rule. One of the key provisions of the HIPAA Privacy Rule is to assure that an individual's health information is properly protected and that individuals can control how their health information is accessed and used. Providing healthcare organization employees as well as patients with smart healthcare cards can help ensure that health information is accessed only by those with the appropriate credentials. Many recent high-profile breaches of protected health information occur because data is kept on unsecured, unencrypted devices such as CDs and USB flash drives, or because entities have been able to access medical records without proper authorization. A smart healthcare card can minimize or eliminate such breaches using embedded secure chip technology, encryption, and other cryptography measures that make it extremely difficult for unauthorized users to access or use information on the smart card or to create duplicate cards. These capabilities help protect patients from identity theft, protect healthcare institutions from medical fraud, and help healthcare providers meet HIPAA privacy and security requirements.

In summary, smart healthcare cards can better position healthcare organizations and providers for meaningful use of EHRs, while addressing many of the security and privacy challenges that come with EHRs and health data exchanges.

III. Smart Cards and Patients

General

1. How can smart healthcare cards help patients?

Smart healthcare cards can help patients in a number of ways, all stemming from the card's ability to authenticate a patient's identity when the patient seeks medical care. Identifying the patient is the cornerstone of quality medical care and good health system management.

Accurate identification of each person who receives healthcare has multiple benefits:

- Decreases medical errors
- Expedites the admissions process
- Reduces healthcare costs
- Expedites claims reimbursement
- Reduces the incidence of medical identity theft and fraud

Optimal medical care requires that a healthcare provider have access to all of a patient's relevant medical history and know what medications have been prescribed. Full access can be challenging, as individuals seek care from more than one healthcare organization and fill prescriptions at more than one pharmacy. A validated patient identity can be linked to a healthcare organization's medical records. Using a smart card also allows the patient record numbers assigned by different medical providers to be stored securely and privately. Other personal information, such as a patient's prescription history, name, address, insurance information, allergies, emergency contact information, and other key data can be stored securely on the card.

Use of a smart healthcare card allows patients to bypass the clipboards, paper work, and lines typical of in-patient admission offices or ambulatory care admissions stations. Instead, when entering a healthcare facility, patients can register by inserting the smart healthcare card into a reader at a kiosk or station. The provider receives the patient's current information and a link to the cardholder's medical records, making the registration and admission process more convenient for the patient. The card's ability to link to and quickly access all of a patient's medical history makes it less likely that doctors will need to order duplicate tests or procedures.

Significant cost savings start at the admissions process and continue through the claims management process. Providing complete and accurate information during the registration process and removing issues caused by a language barrier or human error greatly reduces the incidence of denied or delayed claims.

Medical identity theft and fraud is a growing concern for both consumers and providers. Smart card technology supports the use of additional security mechanisms, such as a photo, PIN, or biometric data (e.g., a fingerprint), preventing the use of a lost or stolen healthcare card by someone else. The data kept on the card can also be encrypted so that no one can access the data without permission.

In short, smart card technology can help patients obtain better healthcare that is delivered faster and more cost effectively.

2. How would patients use smart healthcare cards?

How a patient uses a smart healthcare card depends on the issuer (e.g., insurance provider, hospital, or government-sponsored medical plan) and the applications that the issuer decides to implement. For example, typical uses could include:

- Registering at a physician's office or hospital (Figure 7)
- Securely accessing a personal health record, e.g., to check or update information or schedule an appointment

- Updating personal, insurance, prescription, or medical record information

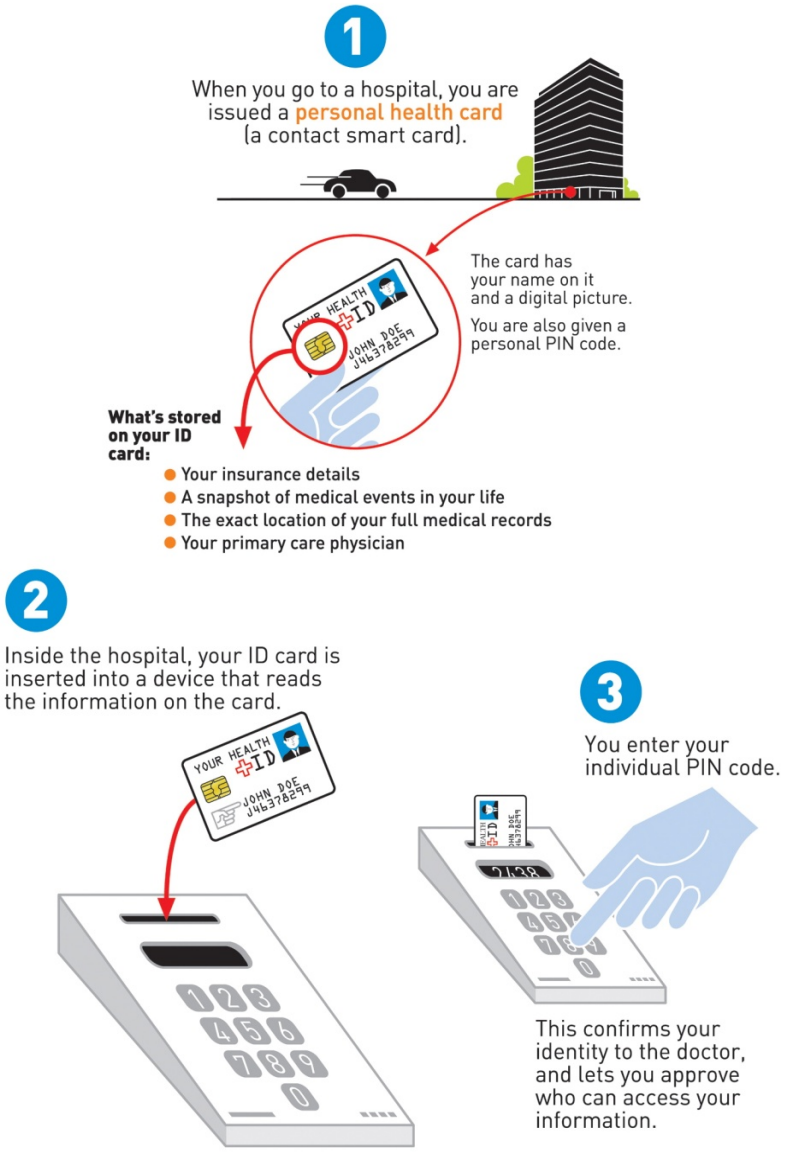

Figure provided courtesy of Gemalto.

Figure 7. How Smart Healthcare Cards Can Work at a Hospital

3. How do smart healthcare cards protect personal healthcare information?

The chip embedded in the smart card can store various types of information. A smart card can protect information using sophisticated encryption algorithms and allow only authorized access; other smart cards may provide a key that unlocks a particular database on a particular computer. Smart card technology also supports multi-factor authentication, requiring the presentation of a second identification factor such as a PIN or biometric data (e.g., a fingerprint) to grant access to personal healthcare information. Smart cards have the capability of providing strong authentication, digital signatures, and security through encryption.

IV. Smart Cards and Healthcare Providers

General

1. How can smart healthcare cards help providers?

Smart card-based systems can support numerous applications and capabilities that are important to healthcare providers:

- Accurate patient identification across organizational and geographic boundaries
- Integration with health information exchange Enterprise Master Patient Index (EMPI) and record locator systems
- Prevention of the issuance of duplicate IDs and ID cards
- Ability to identify all locations (at the healthcare information exchange level) where a patient identifier has been used
- Resistance to counterfeiting
- Risk mitigation for identity theft, data breaches, and fraudulent use
- Support for reporting, quality assurance, and education
- Mitigation of legal and financial liabilities
- Ability to securely store patient identifiers and support deactivation of lost identifiers
- Recording and updating patient demographic data and data copying, data reporting, and interfacing with other healthcare information systems
- Accurate patient identification across the provider network and different systems and acknowledgement of conflicting medical identifiers
- Integrated verification of patient identity using external sources (such as Lexis Nexis or Veratad)
- Multi-factor authentication using photos, PINs, biometrics, and graphical passwords.
- Support for emergency medical services, including providing data to authorized response personnel and tracking patient location during a disaster
- Confirmation of patient identity for Medicaid/Medicare/Children's Health Insurance Program (CHIP) claims
- Verification of insurance, co-pay, deductible, and HSA at time of service
- Payment collection, using the card for a financial transaction
- Automatic check-in at a provider kiosk
- Data audit trails and date stamps at locations used
- Secure, convenient access to patient health information by healthcare providers using smart healthcare cards for identity authentication
- Interoperability with a range of portable devices, allowing healthcare providers to access patient information on mobile platforms/devices or via VPNs

2. How can smart healthcare cards help hospitals?

Smart healthcare cards can significantly reduce hospital administrative costs while maintaining or improving current levels of quality of care and customer service.

Use of a smart healthcare card can benefit hospitals in several ways:

- Improved patient identification
- Increased administrative efficiency
- Improved medical records management
- Improved quality of care

- Increased privacy, security, and confidentiality

Improved patient identification. Real-time verification is a superior method for confirming the identity of an incoming patient, and smart cards can be highly reliable and secure identifiers. The cards can securely store various identity credentials (such as a PIN, photo, or biometric) on the card and make it very difficult to forge or steal the credentials. A smart card can also support digital signatures, which can guarantee that information has not been modified. Smart cards therefore can represent a considerable barrier to medical identity theft and fraud.

Increased administrative efficiency. The time and resources required to admit a patient are critical measurements of hospital efficiency. Busy waiting rooms, thin staffing levels, language barriers, and manual transcription of important data from handwritten forms all create opportunities for error. Smart healthcare cards can decrease the time required for admissions by providing immediate access to accurate, up-to-date patient information. Moreover, the set of information typically provided by the patient can be obtained through an online preregistration process and downloaded onto a smart card. Last, admissions can be streamlined when patients use smart cards at unmanned kiosks, removing the labor element altogether. These efficiency gains can result in lower costs,[18] reduce errors,[19] and improved patient experience.

Smart cards issued for healthcare provider identification can provide secure, affordable remote access to patient health information via a range of devices. As a result, healthcare providers can increasingly access information when/where they need it in a convenient, user-friendly manner.

Secure remote authentication for providers. Smart card technology meets or exceeds recommendations being put forth by the Office of the National Coordinator for Health IT Privacy & Security Tiger Team, providing support for both NIST Level 3 and Level 4 assurance.[20]

Improved medical records management. Linking a patient to that patient's medical records seems like a simple process, but human error often prevents the correct match of patient and records. Using a smart healthcare card to tie a patient to a specific medical record can ensure a more comprehensive and accurate patient health record. Smart healthcare cards can significantly decrease the incidence of and expenses associated with duplicate record creation,[21] improving both administrative functions such as billing and registration and continuity of care.

Improved quality of care. One key benefit of using smart healthcare cards is a potential reduction in the number of medical errors and the quantity of duplicative medical testing. More than 195,000 deaths occur in the United States because of medical error, with 10 out of 17 medical error deaths each year due to "wrong patient" errors.[22] Smart cards can contribute to better care by authenticating the identity of the person receiving medical treatment. The ability to accurately link a patient to an institution's medical records potentially reduces the number of adverse events and medical errors that occur due to lack of patient information.

Increased privacy, security, and confidentiality. Because a smart healthcare card is in the possession of the patient, and because information would be supplied by providers in an "approved" network with audit capabilities, smart cards can provide privacy and security well beyond the requirements of HIPAA regulations. The patient information on a smart card can be encrypted using robust standard cryptography methods that are extremely secure. Smart card technology can also buttress internal hospital security systems. Using smart cards as employee IDs can enable hospitals to limit an employee's physical access to the specific buildings and areas within buildings (including medication

[18] J.Pesce, "Staunching Hospitals' Financial Hemorrhage with Information Technology," *Health Management Technology*, August 2003.
[19] Health Grades, "In-Hospital Deaths From Medical Errors at 195,000 per Year, Health Grades Study Finds," July 2004, http://www.medicalnewstoday.com/releases/11856.php
[20] "How to Authenticate Physicians' IDs," HealthcareInfoSecurity, July 26, 2012, http://www.healthcareinfosecurity.com/how-to-authenticate-physicians-ids-a-4984
[21] Smart Card Alliance, "A Healthcare CFO's Guide to Smart Card Technology and Applications," February 2009.
[22] Robin Hess, "Identity Crisis," *For the Record*, January 17, 2005.

cabinets) that are appropriate for that employee's responsibilities. Smart employee IDs can also be used to authenticate employees for access to networks and computers.

3. Are any hospitals or healthcare systems currently using smart cards?

Countries throughout Europe and Asia are providing their citizens with smart cards. Some use the cards in their national healthcare programs. Others have smart card-based national ID programs. Table 1 lists a selection of smart healthcare card deployments.

Table 1. Examples of Smart Healthcare Card Deployments

Country	Card	Number Deployed	Launch Year
Algeria[a]	CNAS	7 million	2007
Austria[b]	e-card	11 million (patient) 24,000 (professional)	2005
Australia[c]	Medicare Smartcard	40,000	2006
Belgium[d]	Social system identity	11 million	1998
France[e]	Sesam Vitale Sesam Vitale-2	60 million (total)	1998 2007
France[f]	Carte DUO (private insurance card)	Over 200,000	2007
Germany[d]	Gesundheitskarte (health card)	80 million 375,000 professional	2006
Hungary[d]	MOK, Hungarian Chamber of Doctors	40,000	2006
Italy[g]	Carta Nazionale dei Servizi (national service card)	3 million	2004
Kenya[l]	MediSmart Card	300,000	2007
Mexico[h]	Seguro	3.7 million	2006
Slovenia[i]	Health insurance card	2 million (patient) 70,000 (professional)	1999
Spain[d]	Carte Santé	5.5 million	1995
Taiwan[j]	National health insurance card	24 million (patient) 150,000 (professional)	2002
United Kingdom[k]	NHS Connection for Health (health professional card)	1.2 million	n/a

Sources

[a] http://www.gemalto.com/press/archives/2006/07-04-2006-algeria.pdf.
[b] http://www.bellid.com/index.php/content/view/137/73/, http://www.scc.rhul.ac.uk/public/smart2_final.pdf.
[c] Oberthur Technologies, Medicare Australia.
[d] Gemalto.
[e] Gemalto (http://www.gemalto.com/brochures/download/france_health.pdf), Oberthur Technologies (http://www.oberthurcs.com/UserFiles/File/id_vitale2_1108.pdf).
[f] Oberthur Technologies (http://www.oberthurcs.com/UserFiles/File/id_sintia_0808.pdf).
[g] Oberthur Technologies.
[h] http://www.gemalto.com/brochures/download/mexico.pdf.
[i] http://www.gemalto.com/brochures/download/slovene_eHealthcare.pdf.
[j] Giesecke & Devrient GmbH – Health Systems Relying on Smart Cards, Dr. Klaus Vedder http://portal.etsi.org/docbox/workshop/2006/ETSI_CENETEC_May06/Presentaciones/17%20K.%20Vedder%20-Giesecke%20&%20Devrient-%20%20Seguridad%20en%20Smartcards.ppt.
[k] Gemalto and CardLogix
[l] http://www.smartcardalliance.org/articles/2007/04/23/oti-and-smart-launch-medismart-trade-medical-card-solution-in-kenya ; http://www.globenewswire.com/newsroom/news.html?d=214892

In addition to the countries listed in Table 1, smart healthcare card programs are active in China, Finland, Jordan, Poland, and Turkey.[23]

Healthcare organizations in the United States and Canada are also implementing smart healthcare cards to support a variety of features and applications.

- Texas-based Resolute Health Care and Baptist Wellness, both part of Vanguard Health, The Memorial Hospital (North Conway, N.H.), and Santa Rosa Community Health Center (Northern California) are deploying patient smart healthcare cards that use LifeMed ID SecureReg™. In all cases, the cards are used by patients as authenticated identifiers to match them to their individual medical records, store relevant patient information, and pass admissions information into the hospital's admitting software, thereby automating the process.
- Seattle Children's Hospital implemented Gemalto smart healthcare cards for over 4,500 clinicians and IT administrators to support portable multi-factor authentication to authorize user access to hospital servers, networks and VPNs.[24]
- The British Columbia government will start issuing the British Columbia Services Card to citizens in December 2012 (total population of 4.4 million).[25] This card will serve as the de facto health card for British Columbia citizens.

4. How can smart card technology improve critical or emergency care?

A smart card accessed by a portable reader can provide a first responder with vital medical data at the scene or en route to the hospital. Smart cards enable immediate identification of a patient and access to the patient's medical record, even when the patient is unconscious or too flustered to convey the entire medical picture accurately or when language barriers impede effective communication. Patients benefit from more immediate and improved treatment.

Born out of the aftermath of Hurricane Katrina, the American Medical Association (AMA) was awarded a three-year public health translational research grant by the Centers for Disease Control and Prevention (CDC) Office of Public Health Preparedness & Response that seeks to promote the health, safety, and resilience of populations affected by a disaster or public health emergency. The AMA Health Security Card, a smart card, contains essential information for healthcare providers, and local, tribal, and state health departments to identify individuals, meet their immediate health needs, improve access critical

[23] Gemalto and CardLogix.
[24] "Seattle Children's Hospital Deploys Gemalto Strong Authentication Solutions to Protect Network Data," Gemalto press release, February 21, 2011, http://www.businesswire.com/news/home/20110221005486/en/Seattle-Children%E2%80%99s-Hospital-Deploys-Gemalto-Strong-Authentication
[25] http://www.gov.bc.ca/bcservicescard

data, and better obtain surveillance and situational awareness, thereby minimizing morbidity and mortality.

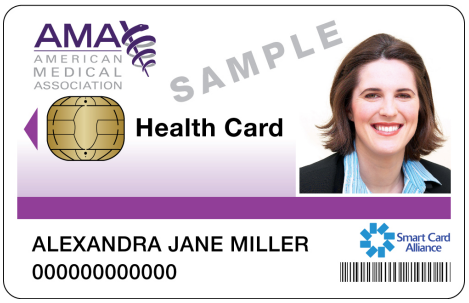

Figure 8. AMA Health Security Card

The Smart Card Alliance served in an advisory capacity to the AMA during the three-year project. In April 2012, FEMA led exercises in San Antonio, TX, comparing the level of care and throughput of casualties in the event of a disaster for patients carrying a health security card versus those not carrying a health security card. Preliminary findings from the pilot exercises showed that 90% of patients using the smart cards rated the care they received as "good to excellent," with 75% affirming care as "very good" or "excellent." The smart card was proven to overcome challenges such as language barriers, unconscious patients and other issues typically faced by first responders. The AMA will publish a final report on the smart card pilot in December 2012.

From a hospital's perspective, smart cards enable effective management and coordination of care, from first responders through the emergency room (ER) and the transition to in-patient care. Additional capabilities available from smart card software vendors enable first responders to forward critical historical data to the ER before arrival, allowing the ER to prepare for and triage patients effectively.

Implementation Considerations

5. What are the IT requirements for smart healthcare card support?

As with any IT project, specific requirements for a smart healthcare card system will depend upon the selected product and scope of the implementation. Patient identity software vendors can scale solutions from a simple configuration with a small IT footprint to integration with the provider's full enterprise environment, including registration, admissions/discharge/transfer (ADT), electronic medical records, and heath information exchange. Regardless, the operational concept and architecture of a smart healthcare card system are straightforward, with implementation at any scale including the following common elements:

- **Cards.** A variety of contact and contactless form factors are available, including cards, fobs, and NFC-enabled smartphones among solutions available today. These may all be generically referred to as "smart cards." (See section I, question 8 for detailed discussion.). Actual card-based solutions incorporating printed individualized information, branding material, or patient photos will require printers designed to deliver cards.
- **Readers.** Many readers capable of reading and updating data stored on smart cards are commercially available. Many have the familiar look of credit card readers and are, in fact, also used in commercial transaction settings. Readers may support contact transactions, contactless transactions, or both. For an illustration of the card reader and transaction process, refer to Section III, question 2, Figure 7.
- **Software and Servers.** Middleware and/or application software is deployed at the point of interaction to facilitate the secure exchange of data between card and reader and to enable user inspection of card data if required. Transaction data is transmitted securely back to the host application or distributed based on enterprise rules to support operations.

6. Is an in-place electronic medical records (EMR) system required to benefit from smart healthcare cards?

A smart card system can be self-contained; it does not have to be integrated with other health information systems. The information stored on the smart card can be read and can identify patients correctly and provide information that a hospital might not have in its database (e.g., a recent prescription or record of care at another facility). Of course, efficiency increases when data can flow from the card into a healthcare provider's EMR system.

7. What are the benefits of using smart healthcare cards with an EMR/EHR system?

- EMR users (physicians, physician assistants, pharmacists, nurse practitioners, nurses) are provided with a simple and more efficient logon process with no need to remember complex passwords.
- Healthcare providers have easy access to all necessary patient health information; therefore, health information is not obtained from the patient's memory, which improves the process of gathering health information.
- The rapid availability of medical information in emergency medicine helps to ensure successful clinical outcomes.
- Smart healthcare cards provide healthcare providers with a means of sharing integrated patient health information. Therefore, patient health information does not need to be transmitted from one physician to another through phone, fax and mail. Fundamentally, smart card use with an EMR/EHR system reduces the risk of leaking confidential patient health records and identity theft, which is possible when using the phone, fax and email as ways to transmit health information.
- Use of smart healthcare cards with EMR/EHR systems reduces the incidence of redundant medical testing and unnecessary hospital admissions.

These benefits and processes are important for health information exchanges (HIEs), as well as EMR/EHR systems.

8. Can smart healthcare cards connect multiple medical record numbers for secure ID verification?

With the addition of available identity software, smart cards can connect the multiple medical record numbers assigned to a cardholder by multiple providers.

9. Can smart card application software integrate into current provider software systems?

Smart card solutions can interface into providers' current software systems, including registration; admissions, discharge and transfer; electronic medical record; electronic health record; and heath information exchange systems, supporting continuity and automation of workflow.

For example, inserting a smart card into a reader can trigger the following events (see Figure 9):

1. The smart card software verifies the identity of the cardholder to the provider and displays a photo on the registration screen.
2. The card optionally prompts for PIN entry or biometric data authentication.
3. The card automatically validates the visit and retrieves the correct medical record with the correct visit requirements, using the provider's current registration software.
4. The card provides an audit trail at all check-in points for reporting to required agencies and for payment or disbursement of funds.

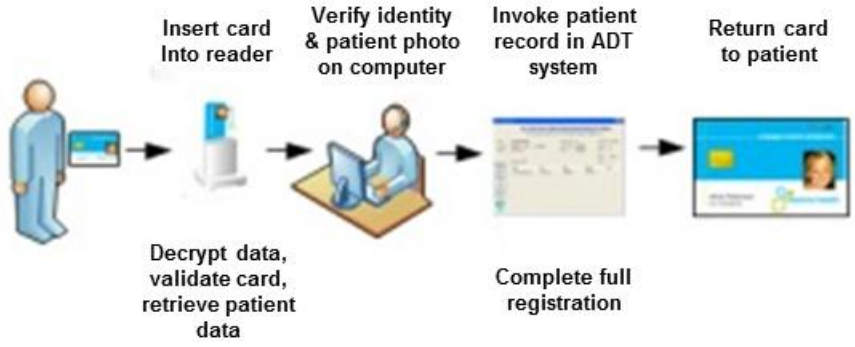

Figure 9. Example Flow for Cardholder Visits to a Healthcare Facility

10. How can patient resistance to a smart card deployment be minimized?

Patients need to know that the smart healthcare card could save their lives. Clear messages should describe to patients the benefits of using smart cards, including the ability of smart card encryption technology to provide high levels of security, support for multi-factor authentication, provision of critical medical information in case of an emergency, and personal ownership and control of access to medical records across disparate groups. Other benefits include the security of knowing that each care visit is managed with the most current and accurate data and that records are not duplicated or incorrectly altered due to data entry errors, language barriers, mistaken identity, or fraudulent use of identity. Cardholders will also appreciate the streamlined and expedited registration process.

Process improvements are also critical for providers who want to increase patient satisfaction scores measured using Press-Ganey scores and internal reporting.

11. How can a patient get a treating physician's records into a personal health record if that physician does not have an electronic health record system?

The following describes an example of how this might be done. An identify software provider can enable any physician with a computer and Internet access to read and write to a smart healthcare card, using a standalone interface that relies on bidirectional HL7 communication or health information exchange interface. A patient can then give that physician permission to access the information on the card to update the patient's personal health record (PHR). When the patient subsequently goes to a provider with access to an electronic health record/PHR exchange, the patient's information can be automatically updated on that provider's system when the card is inserted at any reader or point-of-care station.

Operational Considerations

12. Can one smart healthcare card be used by different providers?

Smart card systems format and exchange data according to accepted healthcare connectivity standards, so there are no technical obstacles preventing adoption of smart healthcare cards by different providers across local or regional healthcare networks. However, as healthcare networks today function at varying levels of technical maturity in adoption and implementation of connectivity, the deployment of smart cards across providers depends most critically upon the goals of the card issuer, business relationships with provider affiliates, and the complexity of provider software systems in the field.

The following are three examples of how this might be implemented.

- Healthcare provider-issued card
- A government-issued card

- HIE implementation

Healthcare provider systems are issuing branded patient smart cards with solution technology providers that connect the smart card across their existing and disparate practice management systems (PMS) and EHRs. The technology also allows qualified first responders remote access to critical patient data in emergencies and natural disasters.

Government and various state agencies are examining ways to increase healthcare's administrative efficiencies and reduce fraud for Medicare and Medicaid, and are proposing pilots that would issue smart cards to replace existing identity cards. Since existing patient smart card technology can seamlessly adapt to existing healthcare provider practice management systems or registration systems, the deployment impact on healthcare providers would be minimal and would noticeably increase administrative efficiencies and influence new revenue sources to help establish a sustainable deployment.

As noted, smart card technology and healthcare systems are based on a number of standards that provide interoperability, and smart cards can be updated electronically as standards may change. HIEs are being implemented across providers and states that standardize data; this may simplify the implementation of smart card technology across providers and existing practice management systems.

The criticality of correct patient identification increases in scenarios involving integration of multiple provider systems and networks. Researchers note that: "As the healthcare industry becomes more computerized and connections are established across multiple disparate systems, challenges increase when matching to a specific and unique person for coordinating that person's healthcare records. The percent of master patient index (MPI) inaccuracies within each entity exponentially increases the number of errors in the HIE environment."[26] The smart healthcare card can play a critical role in closing this medical information gap for a patient and ensuring the right patient is matched to their current medical record at each provider location.

13. Will using smart healthcare cards change an organization's work flow?

Adopting smart healthcare cards may not require an organization to change its workflow. For more on this topic, see the answers to Question 4 on p. 14 and Question **Error! Reference source not found.** on p. **Error! Bookmark not defined.Error! Bookmark not defined.**.

14. Can smart healthcare cards be used offline?

Smart cards can be written to and read when a patient is treated in an offline environment. These capabilities are critical in the event of an emergency or in rural locations with no online access. A healthcare provider can read the card and write to the card, for example, to document medical treatment given.

Business Considerations

15. Who pays for a smart healthcare card?

The issuer of the healthcare card determines who will ultimately pay for the smart healthcare card deployment. While only one entity should pay for the card, all parties involved must accept the solution. The decision can vary by market and scope of deployment.

Adopting smart card technology can add significant value for the provider, not only in terms of improving internal efficiencies, but also meeting new government requirements and adhering to reimbursement or funding limitations. Providers can achieve an excellent ROI for purchasing and issuing smart healthcare cards to patients.

[26] Fernandes, Lorraine, and Michele O'Connor. "Future of Patient Identification." *Journal of AHIMA* 77, no. 1 (Jan. 2006): 36–40. Available in the AHIMA Body of Knowledge at http://www.ahima.org. AHIMA, cited in "Limiting the Use of the Social Security Number in Healthcare." Jeremy Griffin *Journal of AHIMA* 82, no.6 (June 2011): 52-56.

16. What fixed and variable costs are associated with issuing smart healthcare cards?

The costs associated with issuing smart healthcare cards depend in part on what patient identity software solution is adopted. Additional costs can include the costs of integration, customization, the smart cards, printers, readers, cameras, kiosks, and support.

Providers can select a solution with low entry costs. It is also important for the solution to ensure that HIPAA and security requirements are met and to safeguard patient data.

17. Can smart healthcare cards deliver long-term financial benefits to providers?

Card-based solutions have proven to provide robust solutions across a variety of financial, payment, and identity management scenarios over extended periods of time – decades, in fact. The adoption of card-based personal financial transaction tools and standardized transactions sets were significant contributors to economic growth in the last quarter of the twentieth century. The use of secure, smart patient identity cards would not only be sustainable, but would also significantly contribute to reduced operational costs and medical service errors in the healthcare system by validating the identity of the patient at the most critical juncture, the point of the initial encounter.

The National Institutes of Health defines four classes of misidentification errors at patient registration: multiple medical record numbers, wrong patient identification, wrong patient address, and fraud. Misidentification can result from two people having the same or similar names, provision of an incorrect birth date, language barriers, data entry errors, or provision of fraudulent information.[27]

Currently, the process by which identity is authenticated varies, depending on the provider, and often registrars must collect several pieces of information for each patient while processing an average of 200 patients per day. Errors can have multiple consequences with significant monetary and human costs, including duplicate medical records, delayed or denied claims, and medical errors.

According to the American Medical Informatics Association, the existence of duplicate records in a healthcare system is one of the most critical issues currently facing health information technology departments. An average organization's duplication rate is typically between 5–10 percent for a single hospital.[28] A study conducted at Johns Hopkins Hospital found that 92 percent of the errors resulting in duplicate records over the course of a fiscal year occurred during inpatient registration.[29] The prevalence of these errors continues despite decades of systems implementations and improvements, including medical records systems with sophisticated master patient index algorithms. By placing the validated identity in the patient's hands, smart card technology can diminish duplication, reduce cost and improve efficiency by eliminating keystroke errors, and can tie the current medical record to the correct person, ensuring that the same record is retrieved at every visit.

In addition, care can be dramatically improved. Nearly 60 percent of medical error deaths are reportedly due to patient misidentification; based on this, the Institute of Medicine estimates that in 2004, 114,706 people died as a result of "wrong patient" medical errors.[30] Implementing secure patient identity verification and medical information connectivity through smart cards can decrease such untenable and unnecessary costs, reduce medical errors, and enhance overall patient outcomes and experiences.

---

[27] National Institutes of Health, June 7, 2007, 10.1016/j.ijmedinf.2007.04.011.

[28] L.A. Fox and P.T. Sheridan, "EHR preparation: Building your MPI Game Plan," ADVANCE for Health Information Professionals, http://health-information.advanceweb.com/Article/EHR-Preparation-Building-Your-MPI-Game-Plan-1.aspx.

[29] M.J. Bittle, P. Charache, D.M. Wassilchalk, "Registration-associated patient misidentification in an academic medical center: causes and corrections," *Joint Commission Journal on Quality and Patient Safety/Joint Commission Resources,* 2007, Number 33: pp. 25–33.

[30] College of American Pathologists, "Identification Errors," www.cap.org/80/apps/docs/cap/today/feature stories/09051DErrors.html.

18. What is the ROI for smart healthcare cards?

The ROI will vary based on hospital requirements, the savings that are projected (e.g., reduction of errors, productivity improvements, elimination of duplicate records) and the solutions implemented. Some hospitals have realized an ROI in less than a year for a smart healthcare card implementation.[31] For more on this topic and for an example spreadsheet for calculating savings, see the answer to Question 4 on p. 14.

19. What are the implications of smart healthcare cards for insurance co-payments?

Using a smart healthcare card can automate the processing of the patient and the payment. The card can trigger the back-end payment process electronically at registration and checkout to reduce manual keystrokes and improve information quality.

20. What are some approaches for branding and community engagement?

Healthcare providers are interested in their own brands and identity, so branding the card is important. Adding community merchant alliances helps promote acceptance of the technology.

Smart card surfaces, like any other card, can be branded and personalized by the card issuer. Healthcare providers can leverage the card's message and identity by offering the cardholder additional opportunities to the use the card. Examples include providing cardholders expedited access to targeted health and wellness campaigns, or working with local merchants to create alliances that promote the provider's message and engage members of the community. Local merchants may offer discounts or specials when someone shows the branded smart card.

Accountable care organizations (ACO) could use the card to promote and reward healthy behaviors; smart card solutions are available that can track visits across locations. For example, an at-risk patient with a chronic condition could receive points for visiting a wellness clinic or fitness center or keeping a recommended follow-up visit. These patients could redeem these points for "rewards," such as discounts at a gym or a free screening.

Another approach would be an alliance between employers and healthcare providers. The employee's ID badge could also be used as a patient ID and/or insurance card to verify identity at a provider visit, giving the employee automated and expedited service at registration.

[31] Source: Lawrence Carbonaro, "Memorial Hospital: A Case Study," 2009, www.lifemedid.com.

V. Smart Cards and Payers

General

1. How can smart healthcare cards help a payer?

Some of the issues faced by providers are also issues for payers: increased administrative costs, aging accounts receivables, and litigation disputes. HfS Research forecasts a 58 percent increase in healthcare insurance payer outsourcing to reduce administrative costs. Faced with a perfect storm of regulation, spiraling costs, and unprecedented demand, healthcare payers need outside innovation to survive.[32]

Smart healthcare cards and appropriate identity software can give providers the capability to view a patient's eligibility for benefits in real time and accurately determine how much will be reimbursed by the insurer or employer. The provider can then request immediate payment for the visit while simultaneously submitting an electronic claim to the payer. The payer organization, United Health Group, estimates that using automated electronic identity cards to validate eligibility and benefits across the healthcare system would result in $18 billion in administrative savings (fewer key strokes), approximately 50 percent of which would accrue to providers (physicians and hospitals), 20 percent directly to the government in its role as a healthcare payer (through Medicare and Medicaid), and 30 percent to commercial payers, simply by eliminating antiquated manual processes, unnecessary paperwork, and redundant intermediaries.[33]

Fraud alone could be significantly reduced using smart healthcare cards. It is estimated that nearly 1.5 million Americans are victims of medical identity theft.[34] Simply replacing current beneficiary cards with smart cards could eliminate an estimated $30 billion a year in Medicare fraud, according to the Secure ID Coalition.[35]

2. Are any payers using smart cards today?

Using smart cards can have immediate benefits for a payer's bottom line. However, some payers find that there are barriers to adoption of this technology, including lack of consistent data standards, provider reluctance to alter work flows and practices, and lack of development and use of multi-payer applications in professional medical insurance services (PMIS) systems.[36]

Some payers are using magnetic stripe cards and waiting for healthcare providers to adopt smart card technology in order to replace their magnetic stripe cards with smart cards. The provider market is changing. Some healthcare providers are issuing smart cards to patients; the Federal government and some states are reviewing the technology and issuing requests for proposals for Medicare, Medicaid, and children's health insurance recipients. It may be just a matter of time before insurers start issuing smart cards to patients.

The smart card industry is addressing payers' concerns by providing solutions that integrate with current healthcare systems, using cloud-based applications for maximum standardization. In addition, policy makers are suggesting that smart cards replace current beneficiary cards for Medicare patients, stating that proper patient identity would save billions in fraud.[37]

---

[32] HfS Research, "The Healthcare Payor BPO Landscape in 2011 - Will Reform Shatter a Complacent Industry?", August 10, 2011, http://www.hfsresearch.com/node/287.

[33] UnitedHealth Center for Health Reform & Modernization, "Healthcare Cost Containment - How Technology Can Cut Red Tape and Simplify Healthcare Administration," Working Paper 2, June 2009, http://www.unitedhealthgroup.com/hrm/UNH_WorkingPaper2.pdf.

[34] ProtectMyID™, "Medical Identity Theft: The Growing Cost of Indifference," http://blog.protectmyid.com/2011/03/16/medical-identity-theft-the-growing-cost-of-indifference.

[35] Secure ID Coalition, http://upgradethecard.com/.

[36] UnitedHealth Center for Health Reform & Modernization, op cit.

[37] http://upgradethecard.com.

Operational Considerations

3. How is an eligibility check performed with payers?

Eligibility is currently verified by the provider executing a series of laborious manual and electronic processes. Most providers still verify eligibility by phone and fax the night before the patient appointment; others use individual software vendors aligned with payers for eligibility verification.

Using a validated smart healthcare card with multi-factor authentication that works with patient identity software allows for accurate patient identity for each visit and procedure.

4. Can smart healthcare cards handle discrepancies in information in practice systems?

Patient smart healthcare card solutions can store data from multiple sources with a date stamp and an audit trail. This allows a smart card to store a variety of updateable data, allowing the provider to review new and different data and accept or decline such data. Patient smart healthcare card solutions can interface with various provider registration systems and eligibility verification software, enabling providers to review data from other providers, accept or reject the information, and automatically integrate the new data into their current patient record without additional keystrokes or workflow changes.

Business Considerations

5. Do insurance companies pay for the issuance of smart healthcare cards?

The issuer of the health card determines who will ultimately pay for the smart healthcare card deployment. Adopting this technology can add significant value for the insurance provider, delivering improved administrative efficiency and reduced fraud.

It is important to note, however, that while only one entity should pay for the card, all parties involved must accept the solution (i.e., both payers and providers) in order to see the benefits.

6. What are the implications of using smart healthcare cards for copayments, deductibles, payments, and billings?

The use of smart healthcare cards by a claims provider can facilitate electronic claims submissions and couple submissions with the payment capabilities of a credit and/or debit card. Payment can be made in real time. While there is an effort by the Federal government to require that all Medicare and Medicaid claims be filed electronically, no similar mandate exists in the private market. Slightly over 50 percent of insurance claims filed today have an electronic component. Smart healthcare cards bridge the gap from paper to pure digital processing in real time, because they have the ability to store relevant information such as CPT and ICD-9 (ICD-10) codes. Smart cards can also act as a payment source, linking to an HSA or supporting credit/debit payment.

7. What are the benefits of using smart healthcare cards for Medicare and Medicaid?

State and federal representatives, as well as government healthcare leaders, are endorsing the use of smart cards as healthcare cards. Policy makers are advocating that smart cards replace existing beneficiary cards to reduce fraud, including the introduction of Senate bill S.1551[38] to pilot a smart card-based Medicare Common Access Card.

The Office of Management and Budget reported that $54 billion in "improper payments" were made to Medicare ($24 billion), Medicaid ($18 billion), and Medicaid Advantage ($12 billion) during FY 2009. Medicare fraud accounts for an estimated $60 billion in Medicare payments each year. The Secure ID

[38] S.1551: Medicare Common Access Card Act of 2011, http://www.govtrack.us/congress/bills/112/s1551

Coalition has estimated that over half Medicare's annual fraud (approximately $30 billion annually) can be cut by a smart Medicare card.[39] Additional information can be found at http://upgradethecard.org.

[39] http://upgradethecard.com/

VI. Publication Acknowledgements

This frequently asked question (FAQ) document was developed by the Smart Card Alliance Healthcare Council to provide an easy-to-use resource for understanding how smart card technology is used for healthcare applications and for discussing the benefits that smart healthcare cards deliver to patients, healthcare providers and healthcare payers. The FAQ describes potential uses of smart cards in healthcare applications and in patient identity management systems; the features supported and the capabilities of the smart healthcare cards will depend on the specific solution being implemented. Not all solutions provide all of the capabilities discussed in this document.

Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance thanks the Council members for their contributions. Participants involved in the development of this document included: ABnote Group; CSC; Datacard Group; Eid Passport, Inc.; Gemalto; LifeMed ID, Inc.; Oberthur Technologies; OTI America; RM Industries; SafeNet Inc.; SecureKey Technologies; Watchdata Technologies Pte Ltd; XTec Incorporated.

Special thanks go to **David Batchelor**, **Kim Crestelo, Hugh Gilenson**, **Mitchell Hansen, Michael Magrath, Gurpreet Manes**, **Cathy Medich** and **Jim Zalnasky** who developed content for the FAQ.

Healthcare Council members who participated in the development and review of the white paper included:

- **Abrar Ahmed**, Eid Passport, Inc.
- **David Batchelor**, LifeMed ID, Inc.
- **Louis Bianchin**, Watchdata Technologies
- **Kim Crestelo**, LifeMed ID, Inc.
- **Kirk Fergusson**, SecureKey Technologies
- **Anna Fernezian**, CSC
- **Hugh Gilenson**, ABnote Group
- **Mitchell Hansen**, OTI America
- **Dan Hudson**, Datacard Group
- **Brent Iles**, Datacard Group
- **Michael Magrath**, Gemalto
- **Gurpreet Manes**, SafeNet Inc.
- **Cathy Medich**, Smart Card Alliance
- **Bob Merkert**, RM Industries
- **Rick Pratt**, XTec Incorporated
- **John Rego**, OTI America
- **Jim Zalnasky**, Oberthur Technologies

The Smart Card Alliance thanks **Gemalto** for providing graphics for Figures 1, 2, 4 7 and 8 and **LifeMed ID Inc.** for providing graphics for Figures 1, 3, 6 and 9.

About the Smart Card Alliance Healthcare Council

The Smart Card Alliance Healthcare Council brings together payers, providers, and technologists to promote the adoption of smart cards in U.S. healthcare organizations. The Healthcare Council provides a forum where all stakeholders can collaborate to educate the market on how smart cards can be used and to work on issues inhibiting the industry. Healthcare Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects.