*Smart Card Technology in U.S. Healthcare: FAQ Series*

# About Smart Cards FAQ

## In this FAQ



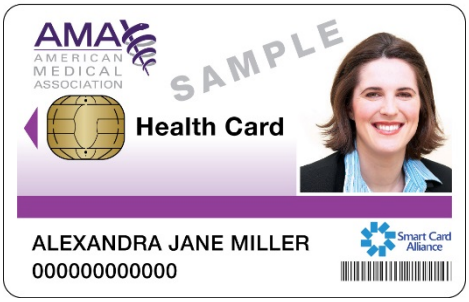
---

### 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 (See question 8). 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. Sample 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 2. Contact smart card technology*

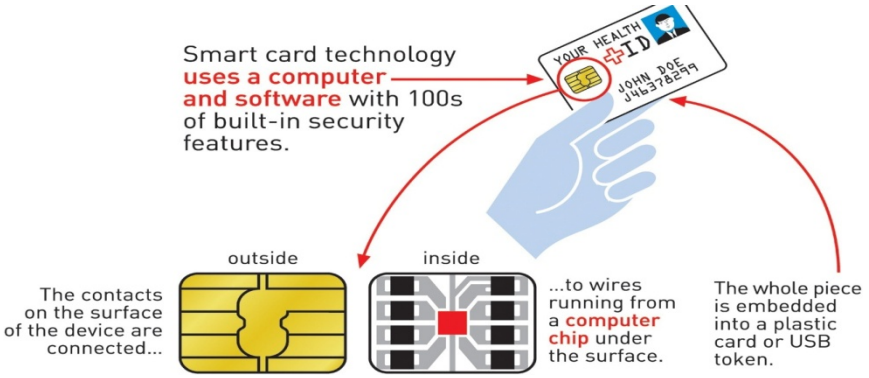



*Figure provided courtesy of Gemalto.*

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 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.

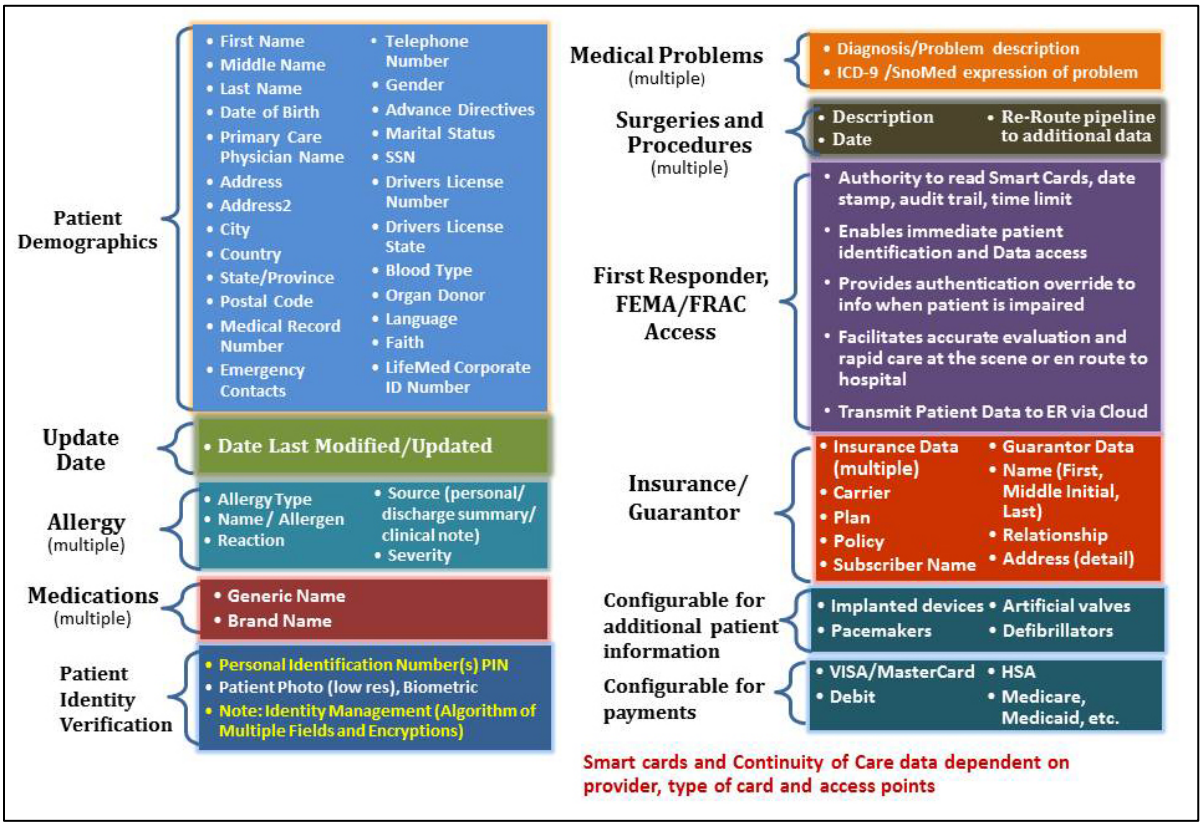



*Figure 1. Examples of the Healthcare Information Smart Cards Can Store*[1]

## 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 multifactor 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.

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

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 specifies that consumer access to online electronic health records warrants the use of multifactor 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.

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.

---

[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.

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

- 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 multifactor 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 Communications (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 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.

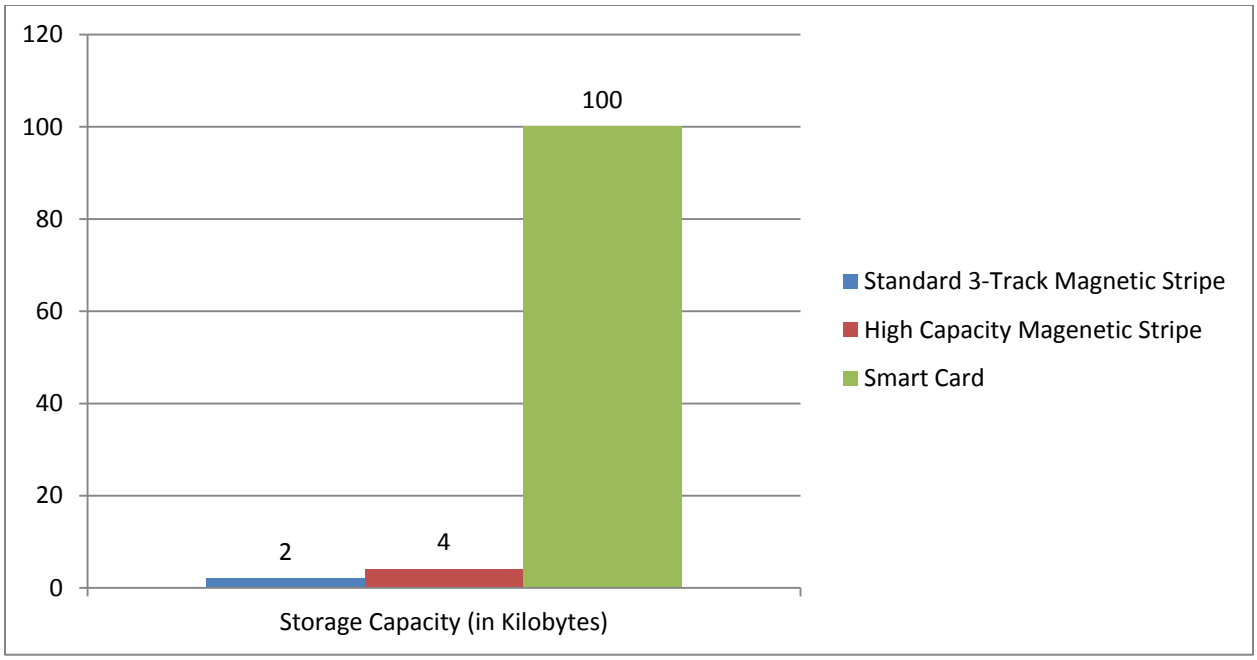



*Figure 4. Storage Capacity of Magnetic Stripe Cards and Smart Cards*

## 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 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. 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, EMT 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 Questions 5 and 6 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-

[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.

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.

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 personal identification number 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.

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.

---

**About the Health and Human Services Council**

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

**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.