A Healthcare CFO's Guide to Smart Card Technology and Applications

A Smart Card Alliance Healthcare Council Publication

.

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 United States and Latin America. For more information please visit http://www.smartcardalliance.org.

TABLE OF CONTENTS

1   Introduction

Healthcare is seeing a steady and increasing dependence on information technology that is rapidly transforming the practice of medicine and the delivery of care.

Technology is an ever-changing and evolving aspect of modern business. In healthcare, most agree that the use of technology is essential to achieving many of the milestones critical to healthcare reform. Three primary drivers are increasing the use of technology in healthcare:

- The need to lower costs and create administrative efficiencies
- The need to improve patient outcomes and enhance physician and patient relations
- The need to meet increasing privacy, security and identity concerns, as a result of Federal and state directives mandating increased control over private information

For healthcare CFOs, the challenge is not only to secure the funding for new technology, but also to weigh the potential benefits of new and emerging technology against the costs. Serious consideration must be given to the consequences of technology adoption for legacy systems, life-cycle costs, and long-term technology evolution.

This white paper outlines some of the major challenges faced by healthcare CFOs and discusses how smart card technology can provide innovative, practical and cost-effective solutions.

2   How Smart Is a Smart Card?

Smart cards first emerged onto the worldwide stage in 1974, when Frenchman Roland Moreno patented a smart card to use as a payment source for a telephone call. Since then, smart cards have found their way into virtually every industry, including healthcare.

Smart cards are essentially miniature computers without display screens or keyboards. Smart cards contain an embedded integrated circuit (or chip) that can be either a secure microcontroller with internal memory or simply a memory chip. The chip is a powerful minicomputer that can be programmed in different ways. Some smart cards hold various types of information in electronic form and protect the information with sophisticated security mechanisms; others provide a key that unlocks a particular database on a particular server. Because of their portability and size, smart cards provide an ideal solution for secure data exchange.

Smart card technology conforms to international standards ISO/IEC 7816 and ISO/IEC 14443 and is available in a variety of form factors, including plastic cards, key fobs, watches, the subscriber identification modules used in GSM mobile phones, and USB-based tokens. Smart cards can perform many functions, such as storing data, making calculations, processing data, managing files, and executing encryption algorithms. Smart cards make possible sophisticated and portable data processing applications and are far more secure and reliable than passwords or magnetic stripe ID cards.[1]

3   Smart Card Use Worldwide

In 2008, 5.045 billion smart cards were shipped worldwide—an impressive 13.2% increase over the 2007 figure of 4.455 billion—with about 15% of these cards entering the U.S. market.[2] While smart cards have had a slower start in the United States, they are now part of a rapidly growing market. Because of their size, flexible form factors (as noted above), and relatively low cost,

---

[1] For an extended discussion of these topics, see the Smart Card Alliance white papers, "Logical Access Security: The Role of Smart Cards in Strong Authentication" and "What Makes a Smart Card Secure?," available at http://www.smartcardalliance.org.

[2] "Worldwide Smart Card Shipments 2008," http://www.eurosmart.com/index.php/publications/market-overview.html.

smart cards are ideal for applications in markets where personal identity, privacy, security, convenience, and mobility are key factors.[3]

3.1   Identification Cards

Smart cards are deployed all over the world for personal, employee, or citizen identification cards, playing a critical role in logical and physical access control systems. Across the globe, public-sector (federal, state, and local governments) and private–sector (financial services and commercial) organizations are recognizing the security and efficiency of smart card operations.

Within the United States, the use of smart cards is growing rapidly within the Federal Government. Homeland Security Presidential Directive 12 (HSPD-12), issued on August 27, 2004, called for the use of a common identification credential for "gaining physical access to federally controlled facilities and logical access to federally controlled information systems." As a result of this directive, a smart card, the Personal Identity Verification (PIV) card, is now being issued to all Executive Branch employees and contractors. Within the next 5 years, 12 million[4] PIV cards will be used in the Federal Government alone.

Enterprises such as Sun, Boeing, Pfizer, Unisys, Lockheed Martin, Northrop Grumman, and others are also implementing smart card-based badges for employee access to both physical and logical resources.

3.2   Payment

Smart cards are used in a wide variety of payment applications.[5]

- Bank card issuers in Europe, Asia, Latin America, and Canada are now issuing smart card-based credit and debit cards that comply with the financial industry's EMV specification.[6]

- In the United States, smart card chips are the core of the contactless American Express, MasterCard, and Visa credit and debit cards that have been issued.

- Smart cards are used in mass transit ticketing and urban parking applications. Within the United States, most major metropolitan areas (including Washington, D.C., Boston, Chicago, Atlanta, Houston, Seattle, and Los Angeles) use smart card-based fare media for transit payment.

3.3   Mobile Telecommunications

Smart cards are used extensively in the telecommunications industry all over the world. According to the GSM Association, there were over 3 billion GSM subscribers worldwide at the end of 2007, accounting for 81.2% of the global market. In addition, there are currently 254 million GSM subscribers in the United States.[7] GSM mobile phones include a subscriber identity module (SIM), which is a smart card configured with information essential to authenticating the phone, allowing a phone to receive service whenever the phone is within coverage of a suitable network.

In addition, over 100 countries use smart cards instead of coins in their pay phones, to improve both customer convenience and the telecommunications operators' business models (less cash, reduced risk of losses). Future applications of mobile phones are expected to leverage the built-

---

[3] Additional information on smart card use in different vertical markets can be found on the Smart Card Alliance web site at http://www.smartcardalliance.org.

[4] Figure provided by the General Services Administration.

[5] Additional information about the use of smart cards for payment applications can be found on the Smart Card Alliance web site at http://www.smartcardalliance.org.

[6] The EMV specification was developed by Europay, MasterCard and Visa to define a set of requirements to ensure interoperability between payment chip cards and terminals.

[7] http://www.gsmworld.com/news/statistics/index.shtml.

in smart card technology and new Near Field Communication (NFC) technology to enable phones to be used for payment and identity transactions.[8]

3.4 Healthcare

Countries throughout Europe and Asia are providing their citizens with smart cards. Some use smart cards as part of their national healthcare programs. Others have smart card-based national ID programs. Table 1 lists examples of national health smart card deployments worldwide; in addition to the countries listed in Table 1, smart health card programs are also active in other countries, including China, Finland, Jordan, Poland, and Turkey.[9]

Table 1. Examples of National Health Smart Card Deployments Worldwide

Country	Card Type	Number of Cards	Launch Year
Algeria[10]	CNAS	7 million	2007
Austria[11]	e-card	11 million patient 24,000 professional	2005
Belgium[12]	Social system identity	11 million	1998
France[13]	Sesame Vitale Sesame Vitale-2	60 million (combined)	1998 2007
Germany[14]	Gesundheitskarte	80 million 375,000 professional	2006
Mexico[15]	Seguro Popular health insurance cards	3.7 million	2006
Slovenia[16]	Health insurance card	2 million patient 70,000 professional	1999
Spain[14]	Carte Santé	5.5 million	1995
Taiwan[17]	National health insurance card	24 million patient 150,000 professional	2002
United Kingdom[9]	NHS Connection for Health (health professional cards)	1.2 million	n/a

---

[8] For additional information on mobile payments, see the Smart Card Alliance white paper, "Proximity Mobile Payments: Leveraging NFC and the Contactless Financial Payments Infrastructure."
[9] Sources: Gemalto and CardLogix.
[10] http://www.gemalto.com/press/archives/2006/07-04-2006-algeria.pdf.
[11] http://www.bellid.com/index.php/content/view/137/73/, http://www.scc.rhul.ac.uk/public/smart2_final.pdf.
[12] Source: Gemalto.
[13] http://www.gemalto.com/brochures/download/france_health.pdf.
[14] Source: Gemalto.
[15] http://www.gemalto.com/brochures/download/mexico.pdf.
[16] http://www.gemalto.com/brochures/download/slovene_eHealthcare.pdf.
[17] 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.

Within the U.S. healthcare industry, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is driving the use of smart cards for both patients and providers to improve the security of healthcare IT systems and protect the privacy of patient information.[18]

Healthcare organizations in the United States are implementing smart healthcare cards to support a variety of features and applications. Prominent programs include the following:

- New York's Mount Sinai Hospital, one of the oldest and largest voluntary teaching hospitals in the United States, has led the trend towards smart healthcare cards. Mount Sinai has joined with nine other institutions in the greater New York City area to create a regional HealthSmart Network that accepts a common smart card-based Personal Health Card (PHC) for regional patients. Elmhurst Hospital (part of the Health and Hospitals Corporation, New York City's public hospital system) is one of the member organizations and a collaborator in the development of the PHC system.

- Texas-based Lake Pointe Medical Center, one of 55 Tenet hospital locations, and The Memorial Hospital of North Conway, NH, are deploying smart patient health cards using the SMART Association, Inc., LifeMed[TM] Personal Health Smart Card Platform. LifeMed[TM] smart cards are issued to patients to more accurately identify the patients, grant them a more streamlined admission, and connect and synchronize patient medical information from sources outside the hospital. Patients with the LifeMed[TM] card have the ability to view and contribute to their overall medical records, giving the provider a more complete medical picture.

- Inland Northwest Health Services, a member of the Northwest Regional Health Information Organization connecting 38 hospitals in northwest Washington and Idaho, is deploying the LifeNexus smart card-based PHC.

4   How Smart Cards Can Improve Healthcare

Over the past few years, smart card use in the U.S. healthcare sector has grown significantly. A number of successful pilot programs have been implemented, some of which are still operational and self-sustaining. Current programs focus on patient identification: streamlining admissions, managing payments, and moving patient data from point to point. Four factors have driven smart card use to date:

- Identification and patient authentication

- Matching patients to their particular data

- Synchronizing data from disparate sources

- Security and access control

Numerous benefits devolve to different healthcare stakeholders from using smart cards. Table 2 lists many of these benefits.

---

[18] Smart Card Alliance, "HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements," September 2003, http://www.smartcardalliance.org/pages/publications-hipaa-report.

Table 2. Smart Card Benefits

Stakeholder	Benefit
Patient	• Positive identification at initial registration • Secure and portable health record • Personal ownership and control of access to medical records • Easier and faster registration • Improved and faster treatment and medical care • Positive identification for payer coverage, treatment, and billing • Accelerated treatment in emergencies • Audit trail through a course of treatment that crosses multiple organizations
Healthcare Provider	• Instant patient identification • Accurate link between patients and institutional medical records • Elimination of duplicate and overlaid records • Faster care delivery in emergency care settings • Rapid accessibility to patient medical history • Potential reduction in adverse events and medical errors due to lack of patient information • Reduction in claims denials • Faster access to key medical record data • Integration with legacy systems with nominal IT costs • Audit trail through a course of treatment that crosses multiple organizations • Reduction in unnecessary/duplicate diagnostic tests or procedures by showing results from other medical providers
Healthcare Delivery Organization	• Accurate patient identity • Reduced medical record maintenance costs (duplicate/overlaid) • Streamlined administrative processing • Increased awareness of provider brand, in and out of the service area • Strengthened voluntary physician/referral relationships • Ability to support value-added service to patient community
Payer (Insurance, Pharmacy Benefits Manager)	• Positive identification of the insured • Verification of eligibility and health plan information • Reduction in medical fraud • Reduction of duplicate tests and reduction in payments • Enforced formulary compliance • Immediate adjudication at point of care • Potential integration with health savings account (HSA) cards
Healthcare Employer	• Highly secure identity credential for both physical and logical access • Single sign-on capabilities (reduction in help desk calls/password management requirements) • Link to other employee services (ID badge, parking, cafeteria)

4.1 Cost Reductions

A major advantage of using smart cards in healthcare is the reduction in costs that results from improving the efficiency of handling medical and administrative information, which also increases the

quality of service. Smart cards support strong authentication of the patient's identity and quickly deliver accurate patient information to the provider. Smart cards can be integrated into current systems and processes within the healthcare industry to provide numerous benefits:

- Secure patient identification.

- Reduced administrative time and cost by automating patient identification.

- Reduced duplication of records.

- Fewer errors and adverse events through the use of accurate and timely information.

- Reduced number of rejected claims and faster payments, by using accurate patient information.

- Reduced fraud and abuse through proper patient identification.

- Reduced claims processing costs through real-time adjudication of claims and insurance coverage verification.

- Increased patient satisfaction, resulting in improved patient loyalty.

As an example, smart cards can facilitate rapid identification of a patient arriving at an emergency room and rapid retrieval of lifesaving information about medical history, recent tests, treatments, and medications. This critical information can be stored on the smart card chip or the smart card can provide secure access to data stored elsewhere. Smart cards can also provide fast access to demographic and insurance information, critical to an accurate registration/admissions process and to downstream billing and payment processes.

4.2   User Authentication and Authorization

Identification, authentication, and authorization are the pillars of security in the electronic world. As the industry moves from paper to electronic medical records, there is growing awareness of the need for secure and encrypted transitional solutions. The National Health Care Anti-Fraud Association estimates that 3% of annual healthcare spending ($68 billion in 2007) is lost due to healthcare fraud.[19]

In addition to the financial loss incurred by healthcare fraud, fraud poses tangible health risks for patients whose records are compromised or manipulated. The case is therefore even stronger for imposing stricter security controls on health information. With the creation of large clinical data exchanges and the ready availability of information on the Internet, all system users need to be properly authenticated before being allowed to access information. System user privileges must be assigned using role-based access controls. And finally, all individuals must have the appropriate authorization to initiate particular transactions.

Smart cards play the critical role, which is properly to identify and authenticate the individual who needs access to a system. If an unauthorized user accesses the system, all other functions fail. Therefore, it is critical that the way in which the user is authenticated be secure.

Smart cards trust nothing until proven otherwise. For example, smart cards can require cardholders to authenticate themselves first (with a personal identification number (PIN) or biometric) before the cards will release any data. And smart cards support encryption, providing patient data privacy and enabling at-home or self-service applications in suspect or untrusted environments to be secure.

The smart card's embedded secure microcontroller provides it with built-in tamper resistance and the unique ability to securely store large amounts of data, carry out own on-card functions (e.g., encryption and digital signatures), and interact intelligently with a smart card reader.

---

[19] The National Health Care Anti-Fraud Association (NHCAA), "The Problem with Health Care Fraud," http://www.nhcaa.org/eweb/DynamicPage.aspx?webcode=anti_fraud_resource_centr&wpscode=TheProblemOfHCFraud.

Smart cards have a long history in the security sector. Governments, financial institutions, and healthcare entities worldwide have recognized the security of smart card systems for user identification, authentication and authorization. Smart card technology is being deployed for international citizen identification cards and within the U.S. Federal Government. In both the security and identity sectors, multi-factor authentication methods have been used aggressively to protect both logical and physical access.[20] It is a natural and much-needed progression for smart cards to provide robust and proven solutions for healthcare.

4.3   Improved Patient Identification and Work Flow

Accurate registration and identity verification can be extremely challenging for hospitals and clinics. Busy waiting rooms, thin staffing levels, and manual transcription of important data from handwritten forms create many opportunities for error. Smart cards can provide positive identification of the patient at the registration desk, by allowing personnel to verify that the patient who is presenting the card matches the photograph on the card or by use of a biometric stored on the smart card.

Using a smart card to verify patient identity can offer healthcare providers the following benefits:

- Make it easy to link patients to the correct medical records

- Reduce the creation of duplicate records

- Reduce the potential for medical identity theft and fraud

- Improve the efficiency of the registration process and the accuracy of data

- Improve the revenue cycle and reduce the number of denied claims

Studies have found that on average, 5%–15% of a hospital's medical records are duplicated or overlaid.[21] This is a serious problem, which many institutions have attempted to remedy with costly and inefficient medical record cleanup initiatives. The flaw in these efforts is that they address the problem after it has occurred rather than addressing the root cause, so duplication continues year after year.

Industry benchmarks place the cost of medical record correction at $20–$100 per duplicate, but these figures can quickly escalate to hundreds of dollars per case when multiple systems are involved and total personnel resources are considered.[22,23] The more duplicates there are in a system, the higher the rate of new duplicates. The growth rate becomes exponential with the size of the patient database.[24]

One manifestation of these issues is the additional cost incurred by an institution. Unnecessary or redundant tests and procedures are often performed due to incomplete or unavailable medical records. In addition, duplicate and overlaid medical records can have dire consequences for patient care and outcomes, exposing an institution to malpractice liability, errors, and adverse events.

Consider, for example, a 300-bed hospital facility with a database of 250,000 patients. If 10% of these records are duplicated (25,000 records), the average cost of cleanup is $500,000–$2,500,000. Unfortunately, without any change in process, this cleanup will need to be repeated every 2–3 years.

By implementing smart card technology as part of the admission and registration process, an institution can reliably identify its patients, increase the accuracy of data capture, optimize patient

---

[20] "The ROI case for smart cards in the enterprise," *Datamonitor*, November 2004.
[21] Madison Information Technologies, Inc., "Medical Record Number Errors: A Cost of Doing Business?," April 2001.
[22] Wheatley, Victoria, "The Significance of the MPI," 2001 HIMSS Proceedings: Workshops.
[23] Just Associates, Inc., "Industry Problem."
[24] Mays, Susan; Swetnich, Donna; and Gorken, Lynda, "Toward a Unique Patient Identifier," Health Management Technology, March 2002.

throughput, accurately link patients to their medical records, and ultimately improve patient experience and satisfaction.

Smart cards can greatly reduce medical record maintenance costs associated with errors from duplicate or commingled patient records. These errors occur when a new record is created for an existing patient, or the wrong patient record is selected. Reducing identity errors during patient registration can also greatly improve billing and collection processes and enhance revenue capture.

4.4   Claims Denial and Revenue Capture

Two of the most common reasons for claims denials are incomplete demographic information and incomplete insurance information, which can cost a healthcare institution millions of dollars in lost or delayed revenue. Most healthcare CFOs are acutely aware of the high cost of reviewing and resubmitting old claims and the revenue lost because of cumbersome claims processing, including detailed chart reviews and outreach to patients and physicians for additional information.

The healthcare revenue cycle is highly dependent on the front-end registration process, which drives much of the downstream claims process. Studies estimate that 50%–90% of claim denials could be prevented by securing accurate patient information at the front desk.[25,26] According to a study by PNC Financial Services, one out of five claims submitted is delayed or denied by insurers, and 96% of claims must be resubmitted at least once.[27] The statistics highlight serious administrative problems that burden providers, payers, and patients. Smart card technology can greatly improve the accuracy of routine data capture. Instead of transcribing information from paper forms and increasing the risk of human error, smart cards can access or provide insurance information, demographics and other patient information, reducing claim denials and increasing cash flow.

4.5   Employee Credentials for Strong Authentication

Smart cards are deployed in hospitals around the world as secure employee credentials. The cards give healthcare providers and hospitals the ability to consolidate a wide variety of functions without compromising on security. Smart cards can be used to authorize physical access, permitting only those personnel who are authorized to enter certain areas of a hospital (such as the pharmacy, operating room, network server room, or human resources). They can also be used to authorize logical access to hospital networks and computers and assist in complying with the HIPAA requirements for privacy and security.

Smart cards provide two-factor authentication, allowing employees to prove their identities in two ways: using something they have (the secure and personalized ID badge) and something they know (their PIN) or something they are (a biometric, such as a fingerprint). Multi-factor authentication provides a higher level of identity verification. In addition, the multi-factor authentication process can be cryptographically protected to assure robust security for corporate network resources.

Smart cards can be deployed easily into existing infrastructures and operate with many industry-leading security applications. Smart card support for standards and interoperability are key advantages for using smart card technology in identification systems.

---

[25] Pesce, Jim, "Staunching Hospitals' Financial Hemorrhage with Information Technology," Health Management Technology, August 2003, http://archive.healthmgttech.com/archives/h0803stanching.htm.

[26] Atchison, Kara, "Surefire strategies to reduce claim denials," Healthcare Financial Management, May 2001, 2003.

[27] Crane, A., "Taking the Offensive against Claims Denials," Hospitals & Health Networks, 81(50): 46-50, May 2007, http://www.hhnmag.com/hhnmag_app/jsp/articledisplay.jsp?dcrpath=HHNMAG/Article/data/05MAY2007/0705HHN_FEA_Payment&domain=HHNMAG.

4.5.1 HIPAA Compliance

The security and privacy of medical records have increasingly been in the news. A recent Harris Interactive Poll[28] estimated that 9 million adult Americans, or 4 percent of the population, believe that they or a family member have lost confidential personal medical information or had the information stolen. The poll suggests that Americans are not only concerned about medical identity theft but are also concerned that their personal information might be violated. Implementing strong authentication within a medical facility will not eliminate but will certainly reduce the risk that personal heath information is compromised.

Adopting smart card technology for use as a secure employee credential for physical and logical access assists with HIPAA compliance for privacy and security. Smart cards comply with the strong privacy guidelines in HIPAA and can be a key component in enforcing a medical facility's privacy and security policies.

Smart cards can provide easier information access management, ensuring that users are following established security policies. Smart cards can help enforce access control to health information, providing support for both user authentication and encryption of data on the card and during transmission.

4.5.2 Benefits throughout the Hospital

Smart employee ID cards deliver benefits throughout the hospital, including:

- Increased operating efficiency and reduced costs. Smart cards provide a cost-efficient alternative to more expensive password-based systems, tokens, and remote access systems, reducing overhead costs and total cost of ownership.
  - Expensive one-time password tokens do not need to be replaced every 3 years.
  - A single identity management system reduces overall infrastructure and redundant technology.
  - Help desk costs are decreased through single sign-on, eliminating the costs associated with requests for replacement passwords.
  - The e-purse capability in smart cards can enable employees to pay for cafeteria, company store/gift shop purchases, parking, and other purchases, making accounting easier and improving employee satisfaction.

- Reduced security application integration time and complexity.

- Reduced security infrastructure and administration. After smart identity badges are issued, they can be activated, updated, and deactivated remotely, not only saving administrative time and funds, but contributing to the security of the institution. For example, if a disgruntled employee is dismissed or leaves the hospital, the smart card can be deactivated, depriving the former employee of access to specific areas, information or records.

- Increased employee efficiency and productivity with self-service capabilities for digital signatures, automatic logon, and secure remote access.

- Easy remote addition, removal, or update of applications. Smart cards offer the ability to add, remove, or change data and applications after identity badges have been issued, eliminating the time and cost of issuing new badges. Applications can range from cafeteria payments to enterprise network single sign-on.

In password systems alone, Datamonitor suggests that an average password related help-desk call can cost an average of $25. For an enterprise with 2,000 employees, these costs amount to roughly $587 per day, $2,935 per week, and $152,620 per year.[29]

---

[28] http://www.harrisinteractive.com/harris_poll/index.asp?PID=930
[29] Zitzer, Aaron, "Why Leading Enterprises are Issuing Employee Smart Cards," IT Today,
http://www.infosectoday.com/Articles/smartcards.htm

4.5.3 Network Security

Hospitals today are enhancing their internal security systems in response to new opportunities and challenges, including:

- Intensified concern about security threats
- HIPAA compliance and other regulatory changes
- Government or industry mandates
- Enterprise-wide desktop computer upgrades and anticipated swap-out cycles
- Standardization or consolidation of physical security systems
- Cost-cutting cycles

Traditional employee badge systems and password-protected network environments can be manipulated to enable unauthorized access. Using smart cards for network security will protect not only patient data but also hospital employee personal data and financial information.

Currently, numerous systems and products are involved in provisioning and managing physical access to facilities and logical access to computing resources and networks, including enterprise directories, human resource systems, proximity readers, policy servers, single sign-on applications, virtual private networks (VPNs), and disk/file encryption. Smart card technology gives hospitals the ability to consolidate a wide variety of functions without compromising on security. The technology also helps increase operating efficiency and productivity, with support for services such as digital signature, automatic logon, and secure remote access. This technology enables hospitals to leverage investment in their current security systems through support for open standards and interoperability with other system components:

- Existing physical security infrastructure can be extended by combining physical and logical access on one badge that is also used for network access.
- Access to applications and data can be managed and protected, regardless of whether the access relies on PCs, the Internet, intranets, extranets, web applications, VPNs, thin clients, or wireless networks.
- Access to and within buildings and facilities at multiple locations can be controlled.
- A comprehensive application can secure employee identity for digital signatures, e-mail, and encryption.
- User and content authenticity can be guaranteed using robust, cryptographic certificates.

4.6 Immediate Access to Lifesaving Information

Everyone in the continuum of healthcare, from ambulance crews to emergency room personnel to physicians and nurses, needs immediate access to accurate medical information such as a patient's medical history, allergies, prescriptions, and over-the-counter drugs. According to a recent study conducted by the Boston Consulting Group, as much as 40% of patient information is missing when needed by a medical professional for proper care.[30] A report published in the *Journal of the American Medical Association* found that adverse drug interactions and medical errors result in an estimated 225,000 deaths per year.[31]

Smart cards carried by patients allow immediate access to vital information and information from other points of care that otherwise might not be available. Even when hospital records are not available, information stored on a smart card or accessed from the smart card with a portable reader provides an easy way to triage patients in emergency and disaster situations. Such

---

[30]Von Knoop C; Lovich D; Silverstein MB; Tutty M, "Vital Signs: E-Health in the United States," Boston: Boston Consulting Group, 2003. www.bcg.com/publications/files/Vital_Signs_Rpt_Jan03.pdf.
[31]"Is US Health Really the Best in the World?", JAMA 2000: 284: 483-485, http://jama.ama-assn.org/cgi/content/full/284/4/483.

information can be accessed from an ambulance en route to a hospital or in the field as part of disaster response (e.g., after a hurricane or other emergency situation). Medical information stored on a smart card can be accessed even when computer networks and power lines are inoperable.

4.7   Healthcare Fraud, Abuse, and Misuse

The National Health Care Anti-Fraud Association (NHCAA) estimates that of the nation's annual healthcare outlay, at least 3% ($60 billion in 2007) was lost to outright fraud. Other estimates by government and law enforcement agencies place the loss as high as 10% of our annual expenditure, or $200 billion, and growing.[32]

A recent Harris Interactive Poll (July 15, 2008) estimated that 9 million American adults (or 4% of the population) believe that they or a family member have lost confidential personal medical information or had it stolen.[33]

The impact of healthcare fraud and abuse reaches far beyond cost; quality of care is compromised by false or inflated claims. The health and well-being of a patient are jeopardized when the patient is exposed to unnecessary and dangerous tests and procedures. Some patients have become "paper pawns" when fabricated histories add erroneous information to their medical records. Fraud can also threaten patients' future insurability.

Smart cards can be used to secure access to electronic medical records. Implementing strong authentication within a medical facility will not eliminate but will certainly reduce the risks that personal heath information is compromised.

4.8   Language Issues and Patient Health Records

Language barriers can hinder information gathering and negatively impact the patient experience. Translation services cannot always provide needed language support, and there may not be time to acquire such services in an emergency situation. Patients may also be unconscious or unable to speak. As a result, healthcare providers are often forced to make critical decisions with little or no information. Smart cards help solve this problem because healthcare providers can access medical information instantly, regardless of the patient's native language or ability to speak.

4.9   Patient and Physician Satisfaction

With higher patient expectations and new levels of competition (such as ambulatory surgery centers, specialty hospitals, and ready clinics), care delivery organizations are seeking ways to differentiate themselves. Patient preferences for and loyalty to a health center or facility are directly tied to impressions of service delivery. Technologies like smart cards can enhance patient satisfaction by improving patient interactions. Smart cards can also help streamline administrative and clinical processes, freeing both clinical and non-clinical personnel to devote more time to patients.

Patients respond to technologies that make them feel more connected to their healthcare, and smart cards provide a way to engage patients directly in the management of their medical information and healthcare events. Smart cards can help patients understand their health information better and provide a tool to help patients communicate their medical information to an array of healthcare providers. Provider organizations are now combining smart cards with kiosk systems and online tools to allow patients to schedule appointments, perform self-service check-ins, and populate common forms.

---

[32]"Financial crimes report to the public—Fiscal year 2006," U.S. Department of Justice, Federal Bureau of Investigation, September 2006,
http://www.fbi.gov/publications/financial/fcs_report2006/financial_crime_2006.htm
[33] "Millions Believe Personal Medical Information Has Been Lost or Stolen," The Harris Poll #74, July 15, 2008, http://www.harrisinteractive.com/harris_poll/index.asp?PID=930.

Smart card programs can also provide value-added services that enhance relations with the physician community and strengthen referral networks. Patients can return to their referring physicians with smart cards containing valuable information about their care (or with the ability to easily access such information), promoting better continuity of care and ultimately better healthcare with lower costs.

4.10   Support for a National Health Network

In 2004, President George W. Bush outlined his vision for a better U.S. healthcare system and called for the creation of electronic health records (EHRs) for every American by 2014. Unfortunately, many experts concede that we are far from realizing a nationwide interconnected health network. While there are many challenges to this vision, the goal is a worthy one and progress is being made.[34]

Federal- and private-sector initiatives have established a framework for the creation of the Nationwide Health Information Network (NHIN). The Office of the National Coordinator is advancing the NHIN as a "network of networks," which will connect diverse entities that need to exchange health information, such as state and regional health information exchanges (HIEs), integrated delivery systems, health plans that provide care, personally controlled health records, Federal agencies, and other networks as well as the systems to which they connect.[35]

The main goal of the NHIN is to develop a scalable and secure system for exchanging healthcare information on a national level. However, implementation of this vision requires a trusted means of validating the electronic identity of both the information requester and the provider. Central to this initiative is the ability to share information among disparate electronic medical records and promote the creation and support of an EHR for every citizen. The ability to establish a secure, private, and interoperable health information exchange is a formidable challenge. Of equal importance is the ability to ensure that the information received does in fact belong to the intended patient.

Because of the highly fragmented nature of medical records and the variability in the use of personally identifying information, the task of unambiguously identifying and linking all of this information becomes exponentially more difficult as the number of sources increases. These challenges are amplified by the fact that we do not have a unique patient identifier in the United States. A recent RAND report highlights these issues as a major challenge to the U.S. healthcare system and calls for a unique patient identifier.[36]

A highly reliable identity management infrastructure is critical to the success and viability of a national network. Smart card technology can play a critical role in this infrastructure. Smart cards can be used to positively identify patients at the point of care and securely track their access to care across multiple providers. The card can be used to aggregate all medical record numbers for a patient as the patient receives care. This can greatly facilitate linkages with local data exchanges and regional health information organizations (RHIOs). Using the smart card in this way greatly improves the fidelity of the linked medical records and reduces reliance on statistical methods for matching patients to medical records, which can propagate errors. Smart cards would also provide access control for those viewing the medical records on the network.

Other advantages to using smart cards as part of a national network are that fraud and abuse can be greatly curtailed, and medical identity theft would be more difficult if an identity credential were part of the process.[37] Additionally, the smart card can be used as a security token for patients to

---

[34] U.S. Department of Health & Human Services, Office of the Inspector General, "FY 2008 Top Management and Performance Challenges," p 39, http://www.oig.hhs.gov/publications/challenges/files/TM_Challenges08.pdf.

[35] U.S. Department of Health & Human Services—Nationwide Health Information Network (NHIN): Background, http://www.hhs.gov/healthit/healthnetwork/background/.

[36] Identity Crisis: An examination of the costs and benefits of a unique patient identifier for the U.S. Healthcare system 2008, http://www.rand.org/pubs/monographs/MG753.

[37] Booz Allen Hamilton, "Medical Identity Theft Environmental Scan," October 15, 2008, http://www.hhs.gov/healthit/documents/IDTheftEnvScan.pdf.

access their personal health records online and can promote greater patient involvement in health and care management.

5 Conclusion

Smart cards provide a valuable and trusted tool for identification and for the privacy and security of electronic information. Smart cards offer extraordinary value to the healthcare sector. They provide a means to an end: using technology to save time, effort, resources, and, most importantly, lives. There are clearly demonstrable returns on investment gained by leveraging smart card technology. They are measurable, they are meaningful, and they address problems that have so far been insoluble. But make no mistake: it is not the technology that is important, it is the result.

Smart cards are portable, secure, and can be leveraged to create closer patient alignments, generate higher patient satisfaction levels, and increase revenue for the healthcare issuer. When there is a win for all of the players and the cost is nominal, technology adoption is rapid and inevitable.

Smart card technology is a reliable and proven solution that has had decades of use in other industries and is now making its mark on healthcare.

6   Resources and References

"Financial crimes report to the public—Fiscal year 2006," U.S. Department of Justice, Federal Bureau of Investigation, September 2006, http://www.fbi.gov/publications/financial/fcs_report2006/financial_crime_2006.htm

"FY 2008 Top Management and Performance Challenges," U.S. Department of Health & Human Services, Office of the Inspector General, p 39, http://www.oig.hhs.gov/publications/challenges/files/TM_Challenges08.pdf

HealthSmart Network web site, http://www.healthsmartnetwork.com/

"HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements," Smart Card Alliance white paper, September 2003, http://www.smartcardalliance.org/download/pdf/HIPAA_and_Smart_Cards_Report.pdf

"Identity Crisis: An examination of the costs and benefits of a unique patient identifier for the U.S. Healthcare system 2008," http://www.rand.org/pubs/monographs/MG753.

"Industry Problem," Just Associates, Inc.

Inland Northwest Health Services web site, http://www.inhs.info/

"Is US Health Really the Best in the World?," JAMA 2000: 284: 483-485, http://jama.ama-assn.org/cgi/content/full/284/4/483

Lake Pointe Medical Center web site, http://www.lakepointemedical.com

LifeNexus web site, http://www.lifenexus.com/

"Logical Access Security: The Role of Smart Cards in Strong Authentication," Smart Card Alliance white paper, October 2004, http://www.smartcardalliance.org/download/pdf/Smart_Cards_and_Logical_Access_Report.pdf

"Medical Identity Theft Environmental Scan," Booz Allen Hamilton, October 15, 2008, http://www.hhs.gov/healthit/documents/IDTheftEnvScan.pdf

"Medical Record Number Errors: A Cost of Doing Business?," Madison Information Technologies, Inc., April 2001

The Memorial Hospital of North Conway, NH web site, http://www.thememorialhospital.org/welcome.html

"Millions Believe Personal Medical Information Has Been Lost or Stolen," The Harris Poll #74, July 15, 2008, http://www.harrisinteractive.com/harris_poll/index.asp?PID=930

Mount Sinai Medical Center web site, http://www.mountsinai.org/

"Nationwide Health Information Network (NHIN): Background," U.S. Department of Health & Human Services, http://www.hhs.gov/healthit/healthnetwork/background/

"The Problem with Health Care Fraud," The National Health Care Anti-Fraud Association (NHCAA), http://www.nhcaa.org/eweb/DynamicPage.aspx?webcode=anti_fraud_resource_centr&wpscode=TheProblemOfHCFraud

"Proximity Mobile Payments: Leveraging NFC and the Contactless Financial Payments Infrastructure," Smart Card Alliance white paper, September 2007

"The ROI case for smart cards in the enterprise," Datamonitor, November 2004

"The Significance of the MPI," Wheatley, Victoria, 2001 HIMSS Proceedings: Workshops

SMART Association web site, http://www.smartassociation.com

Smart Card Alliance web site, http://www.smartcardalliance.org

"Smart Card Applications in the U.S. Healthcare Industry," Smart Card Alliance white paper, February 2006,
http://www.smartcardalliance.org/download/pdf/Smart_Card_Healthcare_Applications_FINAL.pdf

"Smart Cards in U.S. Healthcare: Benefits for Patients, Providers and Payers," Smart Card Alliance white paper, February 2007,
http://www.smartcardalliance.org/download/pdf/Smart_Card_Health_Benefits.pdf

"Staunching Hospitals' Financial Hemorrhage With Information Technology," Pesce, Jim, Health Management Technology, August 2003,
http://archive.healthmgttech.com/archives/h0803stanching.htm

"Surefire strategies to reduce claim denials," Atchison, Kara, Healthcare Financial Management, May 2001, 2003

"Taking the Offensive Against Claims Denials," Crane, A., Hospital Health Network, 81(50): 46-50, May 2007

"Toward a Unique Patient Identifier," Mays, Susan; Swetnich, Donna; and Gorken, Lynda, Health Management Technology, March 2002

"Vital Signs: E-Health in the United States," Von Knoop C; Lovich D; Silverstein MB; Tutty M, Boston: Boston Consulting Group, 2003,
www.bcg.com/publications/files/Vital_Signs_Rpt_Jan03.pdf

"What Makes a Smart Card Secure?," Smart Card Alliance white paper, October 2008

"Why Leading Enterprises are Issuing Employee Smart Cards," Zitzer, Aaron, IT Today,
http://www.infosectoday.com/Articles/smartcards.htm

"Worldwide Smart Card Shipments 2008," Eurosmart,
http://www.eurosmart.com/index.php/publications/market-overview.html

7 Publication Acknowledgements

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.