Testimony of
Kelli Emerick
Executive Director
Secure ID Coalition

Before the
U.S. Department of Health & Human Services
National Committee on Vital and Health Statistics
Subcommittee on Standards
Meeting

Smart Card/Health ID Card Briefing and Discussion
February 28, 2013

919 18th Street, NW, Suite 925 | Washington, DC 20006 | p: 202.464.4000

Table of Contents

Introduction

Thank you, Chairman Green, Co-Chairs Suarez and Soonthornsima, and Members of the National Committee on Vital and Health Statistics for inviting me to present information on the role of smart cards in enhancing health care in the United States. My name is Kelli Emerick, Executive Director of the Secure ID Coalition, and I am here today joined by colleagues from the American Association of Retired Persons and the Medical Group Management Association. We are all here in support of the Subcommittee's development of a plan to create and implement a unified smart card standard that can be used across the healthcare industry to protect patients from identity theft, prevent loss of crucial healthcare dollars from fraud, and promote efficiencies and benefits to healthcare providers.

Founded in 2005, the **Secure ID Coalition** is composed of companies which make smart cards and their attendant technologies. We work with industry experts, public policy officials, and federal and state agencies to promote identity policy solutions that enable both security and privacy protections.

We are here to offer our industry expertise in the area of smart cards, which are used extensively throughout the federal government and around the world to protect access to both physical and logical assets, as well as to protect personal information. In our discussion, I would like to provide information on existing use of smart cards and the benefits associated with them, what kind of benefits that the U.S. healthcare systems would realize from their adoption, ease of implementation and return-on-investment, and current barriers to adoption.

Our healthcare system is under attack. Based on estimates by the Federal Bureau of Investigation, healthcare fraud is costing American taxpayers up to $234 billion annually. Medical identity theft, a small subset of healthcare fraud, costs our economy over $31 billion per year, impacting 1.42 million Americans.[1] For an inside glimpse of how lucrative this type of fraud can be, the World Privacy Forum reports that a stolen medical identity has a street value of $50 – whereas a stolen Social Security number only sells for $1.[2]

The National Academy of Sciences' Institute of Medicine, in its recent report *Better Healthcare at Lower Cost: The Path to Continuously Learning Healthcare in America,* estimated the costs of various healthcare inefficiencies. In 2009 for instance, inefficiently delivered services (mistakes, errors, preventable complications) wasted $130 billion, excess administrative costs squandered $190 Billion, and missed prevention opportunities lost $55 billion. Every dollar wasted is an opportunity lost for healing the sick. We firmly believe that putting into place a framework that allows the nationwide adoption of secure medical identity credentials will save healthcare providers and insurers from losing much needed resources, and in the process, save American citizens from losing their identities, their savings, and in the long run, even their lives.

Smart Cards and the Benefits Associated With Them

I'd like to begin by describing what smart cards are. Smart card technology incorporates a small, embedded computer chip in a card (or other form factor). This integrated circuit chip provides smart cards with built-in tamper resistance and the unique ability to store large amounts of data securely, carry out functions on the card itself, and interact intelligently with a smart card reader.

[1] Poneman Insitute, Third Annual Patient Privacy & Data Security Study, December 2012.
[2] The World Privacy Forum, Medical Identity Theft: The Information Crime that Can Kill You, Spring 2006.

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, fobs, subscriber identity modules (SIMs) used in GSM mobile phones, and USB-based tokens. Smart cards communicate with a reader through either a contact or contactless interface; we recommend using only a contact interface for healthcare uses.[3] In order to work, a contact smart card must be inserted into a smart card reader with a direct connection to a conductive contact plate on the surface of the card (typically gold plated). Transmission of commands, data, and card status takes place over these physical contact points.

Smart cards are used in many applications worldwide, including:

- Healthcare uses – citizen health ID cards, physician ID cards, portable medical record cards
- Secure identity applications – employee ID badges, citizen ID documents, electronic passports, driver's licenses, online authentication devices
- Payment applications – contact and contactless credit/debit cards, transit payment cards
- Telecommunications – GSM SIM cards, pay telephone payment cards

Smart cards have a truly global reach, with over 5 billion smart cards being shipped annually. Smart card-based healthcare ID cards are issued in many countries; France and Germany, for example, have issued over 140 million smart healthcare ID cards to their citizens. Contact smart cards are included in the ANSI INCITS 284 standard for Health Care Identification Cards; the WEDI's Health Identification Card Implementation Guide is also based on this standard and includes smart cards.

Globally, the payments industry has migrated from fraud-prone magnetic stripe bank cards and infrastructure to more secure smart payment cards based on the Europay MasterCard Visa (EMV) specification. Over 1.55 billion smart card-based credit and debit cards are now issued globally and 19.8 million point-of-sale (POS) terminals accept EMV cards as of Q2 2012. Eighty countries globally are in various stages of EMV chip migration, including Canada and countries in Europe, Latin America and Asia. Migration to EMV smart payment cards is now well underway domestically, with U.S. issuers starting to issue EMV credit and debit cards, initially focused on international travelers.

The U.S. Government

The Federal government is the single largest smart card customer, with deployments including the Department of Defense (DoD) Common Access Card (CAC), the Federal Information Processing Standard (FIPS) 201 Personal Identity Verification (PIV) card (with over 5 million issued to all federal employees and subcontractors), and the U.S. electronic passport (with over 75 million issued to U.S. citizens).

In addition to helping reduce fraud costs around the world, smart cards have been a reliable resource throughout the federal government for identity management and security for more than a decade. Designed on open standards approved by NIST, smart cards use non-proprietary technologies to help secure American citizens' identity and security both home and abroad. Most significantly, the DoD CAC card has shown the true security value of the smart card in protecting against fraudulent transactions and unauthorized access. Today every federal agency, including the DoD, utilizes secure smart cards to authenticate and verify users for building and computer access. While it is hard to measure fraud within government agencies, the DoD confirms a 46% reduction in cybersecurity attacks on the first day of secured computer access implementation.

[3] We recommend contact smart card use for a number of reasons. While contact and contactless smart cards are equally secure, many consumers have the perception that a card that can be read at distance can be eavesdropped upon. While this is not true due to the security features on the card, consumer acceptance will ensure robust uptake. Also for practical purposes, Congress is seriously considering a contact Medicare smart card to protect senior citizen privacy and reduce waste, fraud, and abuse within the system. Implementation of a similar contact healthcare smart card would allow doctors and hospitals to use the same reader infrastructure, resulting in additional savings and efficiencies.

International Healthcare

The Secure ID Coalition estimates that healthcare organizations can save over 50% of the cost of fraud based on a number of past smart card implementations throughout the federal government, as well as the international financial services and health care systems. As the US healthcare market is begins adopting smart cards, it also is realizing benefits. A number of nations have implemented smart card-based healthcare systems for many reasons beyond fraud reduction, such as security and ensuring administrative cost savings.

French healthcare system SESAM-Vitale. The French government implemented smart cards in order to verify who was receiving treatment and to quickly provide reimbursements within three to five days as opposed to 3-4 weeks. As a result, the processing cost of a claim within the system was reduced from 1.74 Euros to .27 Euros. With over one billion transactions per year, the transition saves the system over 1.4 billion Euros/year.

German Ministry of Health. Germany deployed secure smart healthcare cards to approximately 70 million beneficiaries and is currently deploying about 280 thousand health professional cards. The projected achievable program savings in the German national program range from 1.7 to 2.9 billion Euros per year, of which between 800 million to two billion Euros would come from fraud reduction. According to the German Ministry of Health in January 2012, the beneficiary deployment alone has generated annual fraud reduction of 250 million Euros. Provider fraud reduction data will not be available until deployment is completed next year.

Taiwanese Healthcare System. The Taiwanese government implemented one of the longest standing and most comprehensive secure health care cards in the world. Implemented in 2004, the program has issued 24 million patient cards and 300 thousand provider cards. The card data includes not only insurance information but medical information as well. The Bureau of National Health in Taiwan reports that moving from paper to a secure smart card has extended the life of cards by 5-7 years, reduced fraud, saved on administrative costs, and reduced health care spending in general. Taiwan's administrative costs are the lowest in the world at two percent (compared to the U.S. at 31 percent).

U.S. Healthcare

While there are myriad examples of smart card implementations in healthcare across the US, we've chosen to highlight two, showing cost savings for both large and small hospitals alike.

Mt. Sinai Hospital, New York City. When Mt. Sinai deployed smart cards to their patients to reduce the number of duplicate or overlaid records in their system, estimated to be close to 15%. The hospital was able to eliminate annual large scale medical record clean-ups which cost the institution $1.8 million and involved over 250,000 duplicate records. Additional benefits included the elimination of the patient clipboard paperwork and reduction in medical errors.

Memorial Hospital, North Conway, New Hampshire. Memorial Hospital reduced admission errors from 6% of patient records to less than 1% by deploying smart cards, including the reduction of medical record error from a rate of 7% to less than 1%, creating an annual savings of $55,000 for a 35 bed hospital. Patients saw a direct benefit as Memorial Hospital was able to reduce their admission time from 22 minutes to less than 3 minutes – an immediate cost savings of $574,000 in annual employee payroll minutes, which allowed Memorial to redirect staff to other productive tasks.

Financial Services

Smart card technology has been used to great success across the globe to protect identity and secure transactions not only in health care, but in the financial services market as well. Known as "Chip & PIN", the smart card technology has revolutionized the way banks have reduced fraud and identity theft. As testimony to their security and efficacy in fighting fraud, American banks have already begun introducing Chip & PIN cards to the U.S. market. Examples of success include:

> United Kingdom Chip & PIN smart card deployment for credit and debit card market. According to a UK Payments Administration reported in 2010, overall fraud losses in the UK fell by 67% and counterfeit card fraud losses have decreased by 77% since 2004, when Chip & PIN was adopted.
>
> France's Chip & PIN smart card deployment for credit and debit card market. The French banking association GIE CB reported in November 2010 that a fraud ratio of 0.072%, for a total 350 million (USD) – of which $140 million (USD) originated outside France. Five years ago 26% of the system wide fraud was attributed to the Internet and 74% attributed to the real world. Today the numbers are exactly the opposite with 75% attributed to Internet fraud and 25% to real world. GIE CB credits smart cards with reducing real world fraud. For a frame of reference, over 3.5 billion smart card transactions occur every year for a value of $597 billion (USD). There are 58 million smart banking cards in circulation in France (population 64m) with an average of 113 operations/transactions per user.

Legislative & Regulatory Factors Encouraging Smart Card Adoption

The healthcare industry is required to comply with a myriad of federal laws and regulations pertaining to the use and storage of patient's personal information, the protection of that information, and now the promulgation of electronic health records and their meaningful use. The one element missing thus far from the regulatory ecosystem is a reliable cross-industry standard that all healthcare providers can use for authenticating and managing the identities of patients, healthcare professionals, and administrative support staff alike. Smart cards are in compliance with the Drug Enforcement Agency's rules for ePrescribing controlled substances. And Congress has strongly suggested the use of electronic cards to aid in the management of identity in the Affordable Care Act[4]. Bi-partisan federal legislation requiring Medicare to undertake a smart card demonstration program has been introduced in both the House of Representatives (HR 2925) and the Senate (S. 1551).

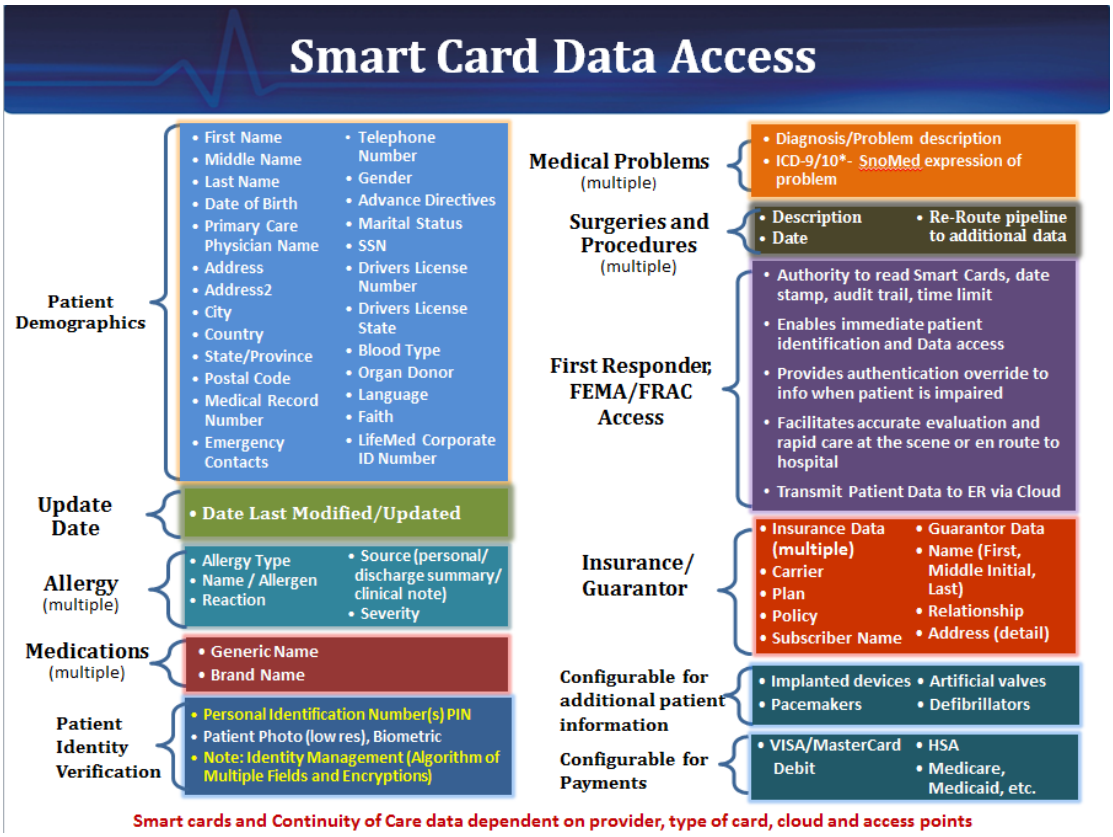
In addition, the individual states are now showing interest in moving to a smart card-based beneficiary identity system; South Carolina recently issued a request for proposals to introduce smart cards in the state's Medicaid system. Combined, we believe that there is clear intent that Congress (and now the states) supports this technology as a means to increase patient privacy and reduce the administrative burden on patients, health care

[4] Section 1104 of the Patient Protection and Affordable Care Act (Pub.L. 111-148) states:

> ''(4) IMPLEMENTATION.—
> ''(A) IN GENERAL.—The Secretary shall adopt operating rules under this subsection, by regulation in accordance with subparagraph (C), following consideration of the operating rules developed by the non-profit entity described in paragraph (2) and the recommendation submitted by the National Committee on Vital and Health Statistics under paragraph (3)(E) and having ensured consultation with providers.
> ''(B) ADOPTION REQUIREMENTS; EFFECTIVE DATES.—
> ''(i) ELIGIBILITY FOR A HEALTH PLAN AND HEALTH CLAIM STATUS.—The set of operating rules for eligibility for a health plan and health claim status transactions shall be adopted not later than July 1, 2011, in a manner ensuring that such operating rules are effective not later than January 1, 2013, and may allow for the use of a machine-readable identification card (emphasis added)."

providers, and health plans. We also believe that, with the NCVHS' assistance in creating an industry-wide standard, this technology will also greatly benefit the healthcare sector with its increasing regulatory burden.

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. This chart illustrates examples of the types of healthcare information that may be stored on a smart healthcare card.

(Chart courtesy of LifeMedID, Inc.)

More Effective Regulatory Compliance

Smart health ID cards can facilitate compliance with Health Insurance Portability and Accountability Act (HIPAA) requirements, especially 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 cards helps to ensure that health information is accessed only by those with the appropriate credentials. Many recent high-profile breaches of protected health information have occurred because data was kept on unsecured, unencrypted devices such as CDs and thumb drives, or because entities have been able to access medical records without proper authorization, smart credentials minimize or eliminate such breaches by enabling strong authentication for information access.

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

HIPAA stimulated the first concerted step toward conversion of paper medical records to computerized records in the U.S. healthcare industry. However, HIPAA provided no clear roadmaps, incentives or benefits for this costly and time-consuming process over the last 15 years, so most institutions and providers made little progress. The HITECH Act of 2009, however, brought change to the industry by focusing on key areas of use of electronic medical records and mandating that healthcare institutions implement new technologies (such as smart card and other technologies). Implementation is to be done under stringent guidelines, which the government will support, both developmentally and financially. Newsweek described this healthcare technology climate change in an online article entitled "The Smart Set."[5]

According to the article, "...two recent changes to health policy will likely push hospitals in the direction of smart cards. First, the stimulus package puts $19 billion toward 'utilization of an electronic health record for each person in the United States by 2014.'" The article goes on to describe how the HITECH Act integrates both incentives and penalties to put teeth in the requirements. "Moreover, new legislation, passed in 2009, steeply increases the fines for patient security breaches. Penalties that used to cap out at $25,000 can now go as high as $1.5 million. Taken together, these two changes push healthcare providers toward a system that is both electronic and secure." The HITECH legislation will require more sophisticated security controls for handling healthcare data. Encryption, two-factor authentication, and biometrics have all been cited as examples of technologies that should be considered to secure and protect healthcare data and systems.

Noteworthy is the fact that smart card technology can be used to implement all of these technologies – and positioned to become such an integral piece of the new healthcare technology landscape precisely because of its ability to assist in meeting meaningful use requirements: providing the technological capability need for providing secure storage and access to EHRs, enhancing and improving EHR functionality and workflows, and ensuring security protocols meet and/or exceed the requirements of certification.

Smart health ID cards will also bridge the gap for several meaningful use measures. The smart health ID card used in conjunction with cloud technology can help an eligible hospital or provider satisfy federal meaningful use requirements by offering solutions for many Stage 1 measures, including electronic provision of discharge instructions, accessibility to patient education; provision of a health information exchange; and provision of privacy and security of electronic health records.

Economic Benefits to the U.S. Healthcare System

While aid and relief from the increasing regulatory burden is an important issue, we believe that the administrative and cost efficiencies brought by a smart identity credential are the other half of the compelling argument in favor of an industry-wide standard. Here's a look, at a glance, on how all stakeholders would benefit.

[5] Newsweek, The Smart Set, February 17, 2010.

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)

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.

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.

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 cards' 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.

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. It is a natural and much-needed progression for smart cards to provide robust and proven solutions for healthcare.

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

While it is difficult to pinpoint the actual cost of duplicate medical records on a healthcare organization, according to Fox and Sheridan, an average organization's duplicate rate is typically between 5–10% for a single hospital.[6] Using their estimate of $50.00 per duplicate pair for an organization in hidden operational costs, a hospital that creates only 5 duplicates a day would end up spending $78,000 per year as a result of duplicates. It is important to note that in this article they used a six day week for their calculations. However, hospitals do not refuse admissions to patients when the health information management staff is not working and searching for duplicates. In other words, duplicates would still be created on the seventh day, and therefore they should be considered in the calculations causing the cost to rise to over $91,000 per year.

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. 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. For instance, in 2005, a Twin Cities' healthcare organization that wished to remain anonymous admitted during a preliminary interview that an external consultant company that specializes in clean-up had been hired. They reviewed 65,000 potential duplicate pairs. They merged 22,000 pairs, but the remaining 38,000 pairs were reviewed and not merged due to missing or conflicting information. This process cost the organization $729,000. If an organization continues to fix the problem as opposed to preventing it, they could end up performing the same costly fixes every few years.[7]

---

[6] Fox LA, Sheridan PT, EHR Preparation: Building Your MPI Game Plan, Advance for Health Information Professionals, February 2004.

[7] McClellan, M., Duplicate Medical Records: A Survey of Twin Cities Healthcare Organizations, AMIA Annu. Symp. Proc. 2009; 2009: 421-425.

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 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.

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.[8] 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.[9] 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.

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.

---

[8] Pesce, Jim, Staunching Hospitals' Financial Hemorrhage with Information Technology, Health Management Technology, August 2003.
[9] Crane, A., Taking the Offensive against Claims Denials, Hospitals & Health Networks, 81(50): 46-50, May 2007.

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.

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.
    - Ease of use and accountability for ePrescribing of controlled substance purposes.
- 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.

Smart cards can also eliminate passwords, the bane of any IT department. In password systems alone, DataMonitor suggests that an average password related help-desk call costs 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.[10]

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.

[10] DataMonitor, The ROI Case for Smart Cards in the Enterprise, November 2004.

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.

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.[11] According to the US Department of Health and Human Services (HHS) Agency for Healthcare Research, adverse drug events (ADEs) result in more than 770,000 injuries and deaths each year and cost up to $5.6 million per hospital, depending on size.[12] The report goes on to recommend that many ADE injuries and resulting hospital costs can be reduced if hospitals make changes to their systems for preventing and detecting ADEs. Anywhere from 28% to 95% percent of ADEs can be prevented by reducing medication errors through computerized monitoring systems,[13] of which smart cards can be an invaluable part. In addition, care can be dramatically improved.

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 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.

Healthcare Fraud, Abuse, and Misuse

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

[11] Von Knoop C; Lovich D; Silverstein MB; Tutty M, Vital Signs: E-Health in the United States, Boston: Boston Consulting Group, 2003.

[12] U.S. Dept. of Health and Human Services Agency for Healthcare Research, Reducing and Preventing Adverse Drug Events To Decrease Hospital Costs, Research in Action, Issue 1, Accessed February 26, 2013.

[13] Ibid.

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 health information is compromised.

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.

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.

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.

Support for a National Health Network

In 2004, the call went out 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.[14]

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,

[14] U.S. Department of Health & Human Services, Office of the Inspector General, "FY 2008 Top Management and Performance Challenges," p 39, 2008.

personally controlled health records, Federal agencies, and other networks as well as the systems to which they connect.

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.[15]

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.[16] Additionally, the smart card can be used as a security token for patients to access their personal health

Encouraging Healthcare Smart Card Adoption

While the benefits of implementing a healthcare smart card system seem evident, the organizations taking the lead in implementing them have been hospitals, which are largely closed-loop systems. One of the barriers to entry for most healthcare organizations is that there are no overarching standards that will ensure interoperability between all stakeholders in the healthcare ecosystem. Imagine a situation where a doctor's office would have thirty different card readers, one for each of the major medical insurers, because they each had a proprietary patient identity management system. Without government leadership to establish a baseline set of patient identity smart card interoperability rules – based on open, publicly available and non-proprietary standards – the U.S. healthcare system, and the patients it serves, will never realize the possible benefits.

We look forward to working with National Committee on Vital and Health Statistics as it investigates the matter and moves forward to ensuring all Americans a safer, more secure healthcare system.

---

[15] Rand Corporation, Identity Crisis: An examination of the costs and benefits of a unique patient identifier for the U.S. Healthcare system, 2008.

[16] Booz Allen Hamilton, Medical Identity Theft Environmental Scan, October 15, 2008.