SMART ASSOCIATION

Smart Cards In Healthcare: A Logical Evolution

A White Paper

Presented by:
Dale Grogan
Director of Smart Card Initiatives
SMART. Association, Inc.

ABSTRACT

Smart cards, or otherwise commonly called "chip" cards, were developed in 1974 as a method to pay for telephone calls without coins. This first 'stored-value' application opened the flood gates to a myriad of uses for this technology. Once considered the vanguard of technology, Smart cards have found their way into mainstream commerce, including healthcare. At the very least, Smart cards can provide valuable, accurate patient information such as name, date-of-birth, blood type, allergies, medications, and medical conditions – crucial information for any healthcare provider. At best, Smart cards can usher healthcare into the true digital age. Healthcare can benefit dramatically from the utilization of Smart card technology as a stop-over on the way to a fully digital industry.

BACKGROUND

Generally speaking, Smart cards are best described as portable mini-computers that can be programmed for a whole host of services. The three most widely accepted uses of Smart cards are: (1) stored value; (2) authentication and access; and (3) data repositories for healthcare. Stored value cards have been particularly useful for creating auditable cashless transactions, such as management of governmentally-sponsored assistance programs including Food Stamps, WIC and TANF programs. With Smart cards, there is essentially no chance to forge or defraud the system as the card's security system is impenetrable. Authentication and access has been a large focus of federal Smart card issuance to over 4,000,000 GSA and military personnel since 2001. In the case of the "Common Access Card" program (ongoing), Smart cards are used as employee badges which allow employees into office buildings as well as allow for computer log-on access. The greatest untapped opportunity lay in the healthcare sector. Modest trials have been undertaken in the past 8-10 years, with various degrees of success. However, it appears the market is ready to engage and embrace Smart card technology as a natural evolutionary step towards becoming a more digital industry.

Within the domestic healthcare industry Smart card technology can provide the following value:

A. Providing access to accurate information on a timely basis;
B. Acting as a portable data repository;
C. Speeding manual processes such as hospital admissions;
D. Managing the information flow within the system-at-large;
E. Reducing fraud; streamlining administrative procedures,
F. Decreasing expenses from patient verification to insurance confirmation;
G. Facilitation of electronic claims submissions;
H. Acting as a payment source (stored value, HSA payments); and
I. Linking disparate data sources in a secure fashion (RHINOs).

A detailed analysis follows below:

A. Perhaps the most important aspect to the delivery of healthcare is gaining accurate baseline patient data. In every healthcare encounter, standard questions are asked by the provider to the patient: "What is your health issue?", or "Give me your patient history," or "Can you get your records from your last doctor?". The issue of patient data within healthcare is that it simply is incomplete and not available to the patient. What's more, the patient cannot be relied upon to be 100% accurate or 100% truthful. Therefore, any provider starts behind the knowledge curve with regards to having accurate patient information. It has been estimated by the GAO that up to 20% of healthcare tests are redundant simply because prior results are unavailable. Smart cards acting as data managers, can alleviate this $300 billion problem.

B. The most robust Smart card can hold 64 kilobytes of information. That is roughly equivalent to sixty pages of single-spaced text; more than enough for a single patient record, notwithstanding images such as x-rays, CT scans, or PET scans. In this age of third-party payers and multiple providers, a patient is not in control of his medical information, nor is it in one single place. A Smart card can act as the primary data repository and can be held by the patient. One of the essential precepts of the 1996 HIPAA legislation was to empower patients and give back ownership of their personal medical information, away from the providers and payers. Having access to a dynamic data repository is invaluable to providers. Baseline data is crucial, but only as a comparison. Providers manage physical change as well as stasis. Therefore, the ability to develop a long-term record is equally as important as reviewing historic data in pieces. Smart cards can hold all of a patient's essential current information as well as giving pointers to where archived information is held.

C. Ask any hospital administrator the least efficient area of a hospital, and the answer is unanimous: Admissions. Each patient admission (small hospitals will admit 10,000 patients per year, large hospitals 60,000) requires patient verification, insurance verification, patient history, and reason for admission. Each of these time-consuming processes can be tremendously foreshortened by having all of that information available on a Smart card. The Smart card would simply be presented by the patient to the admissions clerk. The card would authenticate the user, provide the patient history, and provide access to the hospital's admissions software program. Additionally, Smart card software can aid in preparing standard hospital paperwork such as "Consent-To-Treatment" forms as well as "HIPAA Disclosure Policy" forms, thereby saving additional time, money, and headaches for all involved.

D. As connected as healthcare providers are, they are neither inter-connected, nor intra-connected. Doctors of different specialties, for example, are not electronically connected to each other to securely transmit data. The current state-of-the-art data transfer is still the photocopy machine. Insurance companies are not connected to other insurance companies, the government is not connected to private payers, and the no one is connected to the patient. Inter-connectivity between the vastly different players is totally absent. Worse, connection within a single operator (intra-connectivity) is poor at best. In a large physician group, there is not transparency for movement of patient information. The same holds true even for different floors within a hospital: patient information is simply not mobile enough. Smart cards, with security access tokens which allow access for various trusted sources can make patient data as mobile as the patient, regardless of the number of access points.

E. Fraud can be reduced by authenticating patients and their respective benefits. This was shown in dramatic fashion through use of Smart cards in Wyoming to manage the Women, Infants, and Children (WIC) program. For the "Health Passport" program, fraud was shown to drop to less than 1%, according to program administrator Terry Williams. Fraud represents an $85 billion problem on a nationwide scale according to the National Health Care Anti-Fraud Association.

F. Insurance verification costs roughly $3.00 per patient, per encounter, according to statistics offered by the National Hospital Association. Unfortunately for healthcare providers, there is no on-line clearinghouse service for aggregation of patient insurance. Therefore, each provider must verify at each visit, the validity of coverage. A Smart card can be programmed to search and record usage and coverage, including deductibles and periods of coverage. This saving of time and money rates in the billions of dollars per year.

G. While there is an effort by the federal government to force all Medicare and Medicaid claims to be filed electronically, there is no such mandate in the private market. While slightly over 50% of insurance claims filed today have an electronic component to them, virtually none are entirely electronic. Smart cards are excellent at bridging the gap from paper to pure digital processing in that they have the ability to store relevant information such as CPT and ICD-9 codes. However, they cannot and do not have the capability at this time to track and record all interactions during the claims submission and payment process, owing to the lack of central database management infrastructure.

H. Health Savings Accounts (HSAs) have caught on as insurance vehicles for a certain sector of the population, primarily the younger, healthier cohort. In a typical HSA plan, the patient is responsible for paying 100% of his healthcare coverage costs up to a (high) deductible, perhaps $2,500. Currently HSA payments are made as credit or debit payments from an associated HSA account, held at a bank. However, there is no real policing of how the account dollars are spent, even though they are tax-advantaged. Smart cards could effectively be used as stored value devices whereby only approved vendors could accept the stored value (i.e., an approved pharmacy would have a Smart card reader, compared to a gas station that would not).

I. The idea of having a massive on-line central data repository (a Community Health Information Network, "CHIN") has been around for nearly 20 years. The current iteration, called a Regional Health Information Network Organization ("RHINO"), is still an attractive, but much more achievable notion. The issue for viability was providing secure access from the providers as well as verification of the patient. Technology has resolved the security issues; the challenge now is working through the political minefields associated with substantial players sharing proprietary information. Control by the individual provider is lost. While this model of community or regional databases would be optimal in a single payer environment (as is the case in Germany or France, for example), the likelihood of that model developing domestically is minute. However, Smart cards can play a strong role as an interim step down that path.

Each of these benefits decreases the administrative costs within the healthcare system. Moreover, better patient outcomes can be achieved through better information.

So why haven't Smart cards taken over as the default technology in healthcare data management?

1. The cost of replacing infrastructure is relatively high.
2. The current system is not so broken that it totally fails.
3. The providers have the enviable position of controlling patient data and are wont to give up that position.
4. In a data sharing model, too many players would have to cooperate for others' benefits.

SMART CARD TECHNOLOGY

Smart cards are credit-card sized pieces of plastic with an embedded computer chip. The chip can be programmed to perform various functions just as a desktop computer can. Since their development in 1974, Smart cards have become much more sophisticated in terms of applications, and much more robust in terms of storage capabilities. There are over four billion Smart cards in worldwide use today.

There are two types of computer chips on Smart cards:

- A memory chip that simply stores raw information in bits and bytes. These were the first types of chips developed and lacked much security. Typically memory cards have not been updatable. That means, that once a data set has been burned to the memory it cannot be updated or manipulated. The analogy is that a memory chip is like a CD; once it is written, it cannot be re-programmed, but can be accessed many times.
- A microprocessor chip is today's standard. The microprocessor chip has on-board logic sufficient to create its own internal security authentication procedures, along with the ability to secure all or part of its data through encryption techniques. Microprocessor cards have the ability to be read and re-written, making them dynamic. For example, in a healthcare environment, a microprocessor card can maintain up-to-date medical information and be revised infinitely.

For data to be read from a Smart card, it needs to interact with a Smart card reader. Currently, there are two ways a reader can read a Smart card:

- Through physical contact. A contact reader requires the Smart card to be physically inserted into the reader. This is perhaps the most conventional method, and most widely distributed, due to cost. The card goes into the reader, the reader makes an inquiry to the card, the card responds, and the transaction initiates.
- The other type of reader is contact-free. A contact-free reader operates via radio frequency ("RF"). In this case the Smart card has an antenna embedded in the edges of the card, which listens for RF calls from a reader. The range of interaction is up to three inches, but is typically much faster.

Smart cards are governed by several international standards organizations such as ISO/IEC, ANSI in the United States, EMV for payment standardization, and HL7 within domestic healthcare. Additionally the federal government established a series of guidelines for implementation through the General Services Administration ("GSA"). The GSA Interoperability Standards govern the relationships between cards (manufacturers), readers (manufacturers) and applications (developers). All vendors who supply Smart card solutions to any federal agency must comply with the interoperability standards.

The primary uses for Smart cards are:

- Financial transactions. Stored value, or "e-purse" applications are much more prevalent internationally than in the United States. This is because of the premier telecommunications infrastructure domestically and the use of credit and debit cards. Stored value is particularly valuable to prevent fraud and credit alternative forms of currency such as loyalty dollars or coupons.
- Security. Being able to verify the cardholder independently is of tremendous value to employers, governmental agencies, and any entity seeking to protect assets. Smart cards are used as identification cards to grant physical access into building as well as logical access to log onto computers. Many passports now contain Smart chips with individual's data. Because the cards cannot be hacked, immigration agencies can trust the veracity of the card.
- Healthcare. Over 150 million Smart cards have been issued for healthcare applications worldwide. The two leading issuers are Germany and France, who have nationalized healthcare. Smart cards are used as identifiers and data storage units. Domestically, Smart cards have been successfully deployed to (1) Streamlining hospital admissions, (2) Contain demographic and medical information for authorized providers, (3) Maintain emergency and medical directive information, (4) Act as membership loyalty cards, and (5) Manage government healthcare entitlements.
- Telecommunications. The Subscriber Identity Module ("SIM") chip in every cellular phone is a Smart chip. The Smart chips are used to provide unique phone information, storage of applications, as well as store individual telephone numbers. Almost every pay phone in Europe (and now many in the States) is outfitted to accept Smart cards for payment.

INDUSTRY ANALYSIS

Domestic Healthcare Administrative Issues

- A landmark Price Waterhouse Coopers study compiled for the American Hospital Association stated that:
  - For every hour of patient time spent in an emergency room, one hour of paperwork was required; for surgery and in-patient care, 36 minutes; for home healthcare, 48 minutes; for skilled nursing care, 30 minutes.
  - A Medicare patient treated in an emergency room is required to sign eight separate forms – for Medicare alone;
- In 2002, according to The Access Guide (April 2001), administrative costs account for between 40 cents of every dollar spent on healthcare in the United States.
- Lack of complete information on patients contributes to the death of 140,000 hospitalized individuals every year from adverse drug reactions.
- Medical errors are responsible for injury in as many as 1 out of every 25 hospital patients (AHRQ, the government agency for health care policy and research).
- Errors in health care have been estimated to cost more than $5 million per year in large teaching hospitals alone.
- Preventable healthcare-related expenditures cost the economy from $17 to $29 billion each year.
- While there are no data standards for interchange, the ANSI-approved group, Health Level 7 ("HL7") has established widely accepted data messaging standards, paving the way for more and more electronic data transmission through the healthcare industry.

HIPAA Mandates

The Health Insurance Portability and Accountability Act of 1996 intended to cede control of patient information from the provider to the patient. It was intended to help the patient gain access of disparate medical records and to force a movement toward digital medical records. Lastly, it was intended to protect the patient's sensitive data from unauthorized viewing, even within the healthcare industry. The jury is out as to whether the intended consequences were achieved. What is known for sure though is that the HIPAA mandates have created a window of opportunity for the Smart card technology platform to establish itself within the US healthcare industry by fulfilling the security and privacy requirements imposed on the US healthcare sector by HIPAA, and by assisting in digitalizing/automating and thereby streamlining administrative procedures.

- The HIPAA standards govern the uniform electronic formats and codes for claims and related transactions, establish national identifiers for providers, payers, employers and patients, and set forth procedures to ensure the security and integrity of all electronic health data. These requirements are congruent with the functionalities the Smart card technology platform provides. The national patient identifier may be stored on the Smart card where its security will not be compromised. The smart technology could also fulfill the required security and privacy requirements.
- HIPAA is aimed at making the healthcare industry more efficient by replacing the mountains of paper-based health forms with electronic messages. At the same time, the federal government is implementing rules to make sure patient data is kept confidential for the required levels of security and privacy HIPAA demands.
- The HIPAA data security rules cover all electronic health data, whether it is transmitted over public or private networks or even if it never leaves a desktop computer. This means the health information in registration, point-of-care, laboratory, pharmacy, discharge, utilization review, claims adjudication, plan enrollment and many other information systems must be protected by technical mechanisms and administrative policies.

- The HIPAA rules do not require healthcare organizations to electronically transmit or receive claims and related transactions. But under the rules, those organizations that transmits or accepts transactions electronically must use Version 4010 of standard formats from the American National Standards Institute ASC X12N subcommittee. In addition to standard formats for institutional, professional, dental and pharmacy claims, HIPAA requires standards for: claims status, enrollment and dis-enrollment, insurance eligibility verifications, health plan premium payments, payment and remittance advice, and referral certification and authorization transactions.
- Pharmacy claims must conform to national, standard formats from the National Council for Prescription Drug Programs. In addition, the proposed rules require that all transactions use standard diagnosis and procedure codes.
- Even if an organization is not doing a HIPAA-referenced transaction electronically, it may have to comply with the mandates. For instance, if an insurance company provides eligibility verification or referral authorization services by fax, phone or on paper, it must be prepared to accept standard electronic formats of these transactions from any provider that wants to communicate electronically.
- The codes on physician and hospital claims that describe specific treatments and services have also gotten reworked. That means that providers, payers, claims clearinghouses and software vendors have to implement the new codes in their practice management, claims adjudication, decision support and analysis software. The mandated drug codes are twice as long as the former codes and virtually all physician practice management systems have needed modifications.

Electronic Claims Submission

Electronic claims submission, or rather lack thereof, provides a huge void, and therefore opportunity, which the Smart card technology platform can help fulfill by streamlining the entire procedure. Healthcare Smart cards projects in Europe, France and Germany in particular, have long provided claim submission functionality.

- For nearly two decades, the nation's pharmacies have cooperated to develop standardized Electronic Data Interchange ("EDI") and electronically submit nearly 90% of prescription claims. But just slightly more than half of all other claims from hospitals, dentists, physicians and other professionals are electronically submitted.
- Although large payers benefited from the continuing trend of physicians consolidating into larger group practices, commercial insurers accepted only 45% of claims electronically in 1999 (compared with 40% in the previous year). Commercial insurers are private corporations other than Blue Cross/Blue Shield plans that offer a number of products, including HMOs, PPOs, point-of-service plans and indemnity insurance.
- In 1999, HMOs accepted only 18% of claims and encounter reports electronically, compared with 17% the previous year.
- Most smaller commercial payers and HMOs continue, in general, to accept less than 20% of their claims electronically. Many have yet to accept their first electronic claim.
- Providers submitted 64.5% of claims electronically in 1999, an increase of 4% from 1998's rate of 62%.
- Hospitals and pharmacies continue to be the provider leaders in their use of electronic data interchange. Pharmacies inched up their percentage of electronic claims submission to 88.5% in 1998, compared with 88% the previous year.
- The percentage of prescriptions that are paid out of consumer's pockets fell from 37% in 1996 to about 21% in 1999, according to Scott-Levin Inc., a Newton, Pa-based pharmaceutical research firm.

- The percentage of claims physicians and other professionals submitted electronically rose nearly 9% during 1999 to 43%.
- The U.S. Department of Health and Human Services rules require that electronic transactions comply with Version 4010 of standards from the American National Standards Institute X12N subcommittee.

Despite economic pressures, a growing number of Healthcare organizations are devoting more funds in the years ahead to a number of technologies that could enable them to become more efficient. Among these are computer-based patient records, systems and Internet technologies. Hospitals and integrated delivery systems want to offer physicians easier access to clinical records, as well as treatment guidelines. As a result, many organizations will invest in inpatient as well as outpatient electronic records systems that give physicians instant access to data they can use to make appropriate treatment decisions. Smart card based solutions will be able to meet and surpass the security requirements such solutions will demand.

CONCLUSIONS

Smart card technology fills an urgent need in today's complex healthcare environment. Most patients have a primary care physician who maintains medical records of the patient. When referred to specialists or to a hospital, copies of pertinent records are made and sent along with the patient, or separately, in advance. Generally, each medical facility will ask the patient to complete a medical history, with a list of current medications being taken, personal and insurance data, emergency numbers and so forth. Older patients may not know what medication they are taking, may not understand, or may not remember significant health problems from their past, requiring assistance by a nurse or medical technician.

With greater and greater specialization, it would not be unusual for one patient to have records in five or six different places. This makes collecting accurate historical data almost impossible. Additionally, patients are often in need of emergency response services. In these instances, medical records are impossible to access and very seldom do you find anyone around that has the critical information that is required to ensure that the patient receives the highest quality of care possible. Through the use of Smart card enabled solutions, critical information is made available to patients and caregivers instantly, securely and privately in order to dramatically increase patient care as well as improving the overall efficiency of the processes required by the caregiver.

Many believe that by empowering the patient with the information they need when the need it the most it will greatly impact the overall treatment process and help to ensure accurate and efficient care. Many times physicians find themselves relying on the information given to them by patients regarding medications, allergies and past medical conditions that the patient may be able to recall at the time of care. Smart cards significantly reduce the opportunity for human error by allowing the individual patient to securely store current and past medical information on the card and share that information with medical staff at selected points of care providing a potential life-saving benefit and convenience to the physician as well as a to the patient.

Without question, the optimal infrastructure design is a national (or regional) central data network where all healthcare providers, payers, and patients can add and review patient data once they are authorized. This vision would require huge up-front investment, cooperation from all parties, and strict regulations. The dividends would be enormous in terms of dollars and lives saved. This ideal vision is not likely to be seen completely; however Smart cards can aid in moving the mountain stone-by-stone by orderly transition, while creating value at each step.

SMART
ASSOCIATION

198 Cirby Way, Suite 180
Roseville, CA 95678
Toll Free 1-888-550-6550
Fax 916-677-8420
info@smartassociation.com
www.smartassociation.com