Smart Card Applications in the U.S. Healthcare Industry

A Smart Card Alliance Healthcare Council White Paper

Publication Date: February 2006

Publication Number: HC-06001

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org
Telephone: 1-800-556-6828

About the Smart Card Alliance

The Smart Card Alliance is the leading not-for-profit, multi-industry association of member firms working to accelerate the widespread acceptance of multiple applications for smart card technology. The Alliance membership includes leading companies in banking, financial services, computer, telecommunications, technology, health care, retail and entertainment industries as well as a number of government agencies. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information, visit http://www.smartcardalliance.org.

Table of Contents

1 Introduction

John Taylor walks into the cancer clinic with his 7-year-old daughter for what he hopes will be the last time. After almost 18 months of treatment, Rebecca seems to be in full remission. John is relieved—in fact, almost everyone involved is relieved. During Rebecca's ordeal, various family members have filled out the same forms 73 times and been asked the same questions during all 116 visits to the different participating members of Rebecca's care team. Rebecca has received the wrong medication three times (once with dire effect) and been subjected to duplicate lab tests and radiology studies because previous test results were not available. Rebecca's reward for having experienced all this and survived? Expenses of about $18,000 dollars above and beyond what was necessary for her treatment.

Although this story may sound like fiction, it is true. Healthcare systems in the U.S. are burdened with paperwork, prone to errors, and in some cases, hazardous to one's health. On top of these issues, the industry faces high costs, increased fraud and government-mandated requirements to put in place processes and systems that protect the privacy of patients' personal information.

Healthcare organizations are now investigating and deploying new information technology that is designed not only to solve the significant challenges that the industry is facing, but that also provide new functionality that improves patient care and the efficiency of healthcare delivery. Smart card technology is being incorporated into many of these new healthcare systems as an instrumental component that protects and enables convenient access to patient data and that supports new applications that deliver both clinical and administrative benefits.

Smart cards are used worldwide for many applications, including healthcare, financial, transit, telecommunications, and secure identification. Defined at the highest level, a smart card is a device (e.g., a plastic card) that includes an embedded integrated circuit (IC) chip. Applications that use smart cards take advantage of the technology's ability to provide secure, portable data storage, enable authenticated information access (either on the card or within the application system), and support secure transactions between the card and the system. Also important in many applications is the familiar form factor – a plastic card – that is convenient to use.

Smart card technology provides a feature-rich, flexible platform for healthcare organizations to implement applications that address key industry issues. This white paper provides an overview of how smart cards are used in a variety of these applications, including:

- Supporting privacy and security requirements mandated by HIPAA
- Providing the secure carrier for portable medical records
- Supporting new processes that can reduce administrative costs
- Reducing healthcare fraud
- Providing secure access to emergency medical information
- Providing support for patient loyalty programs
- Enabling compliance with government initiatives and mandates

About this White Paper

This white paper was developed by the Smart Card Alliance Healthcare Council to describe the value that smart cards deliver in a variety of U.S. healthcare applications. Developed as an educational overview for executives and senior managers in healthcare provider organizations, it reviews key challenges that the U.S. healthcare provider industry faces and examines the key drivers for implementing smart card-based systems to address these challenges.

The white paper concludes (Appendix I) with profiles of a number of organizations who are implementing smart cards, including Queens Health Network, University of Pittsburgh Medical Center, St. Luke's Episcopal Health System, Florida eLife-Card, Texas Medicaid, and the French and German health cards. These implementations illustrate the diversity of applications that are enabled by smart card technology and the business benefits that the technology delivers to healthcare organizations.

2 Drivers for Using Smart Cards

2.1 Meeting Privacy Requirements

The protection of each individual's medical information is a key concern for patients and healthcare providers alike. Stringent Federal legislation, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), strengthened the requirements for maintaining the security and privacy of patient health data. This government-mandated healthcare reform was originally intended to make it easier for individuals and small businesses to obtain and retain health insurance during job transitions. To help reduce insurance costs, HIPAA has encouraged the use of electronic transactions and requires that all information that is transmitted or stored be kept secure and private. HIPAA applies to all health plans, healthcare clearing houses, and healthcare providers, including hospitals, medical groups, and physicians.

Under HIPAA, healthcare providers are responsible for implementing policies that protect against the misuse, modification, and disclosure of an individual's health information. Patients now have greater control over who has access to their information, while organizations must institute adequate safeguards to shield the privacy of patient information. Civil and criminal penalties hold violators accountable for failing to guard their patients' privacy rights.

Many technologies can be used to provide secure, authenticated access to healthcare information, including technologies that secure both physical and logical access. Systems that use smart cards have distinct benefits. Smart cards have a unique ability to make information access easier for users, while at the same time enforcing the more robust security policies required of healthcare organizations to bring their environments into HIPAA compliance. For example:

- Smart cards can provide easier information access management, ensuring that users are following established security policies.
- Smart cards are a familiar form factor that can be used for both physical access to facilities and logical access to information on personal computers and networks.
- Smart cards can help enforce role-based access control to health information, supporting both user authentication and encryption of data on the card and during transmission and ensuring that individuals accessing patient information see only the information that they are authorized to view while all other information is kept private and secure.
- Smart cards can store health information on the card, performing as secure portable data carriers that are under the control of the patient and the healthcare professional.
- Smart cards, with on-card intelligence and processing capabilities and the ability to use standards-based cryptography, are uniquely capable of enabling compliance with strong privacy guidelines and of enforcing the privacy and security policies set by healthcare organizations.

Smart cards provide a feature-rich platform for healthcare organizations to implement new applications that improve access to and convenience of medical care.

HIPAA and its implications for the healthcare community are discussed in detail in the Smart Card Alliance white paper entitled *HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements*, available at http://www.smartcardalliance.org.

2.2 Supporting Portable Medical Records

Today, managed care, specialized medicine and continual changes in healthcare insurance coverage have fragmented the U.S. healthcare industry and significantly affected patient loyalty. It is not unusual for each patient in a given family to see multiple physicians over time. Since each physician maintains a separate medical file on the same set of patients, this nomadic behavior leads to a dispersion of semi-complete and irreconcilable medical records in various

locations. Indeed, U.S. medical documentation tends to be scattered across multiple media and locations: digitized healthcare records on insurer computers, disks or tapes at hospitals, patient folders at clinics, and prescription files at pharmacies. The national mobility in the U.S. compounds the problem. About one in five Americans moves each year; people change jobs, and employers juggle health plan options trying to balance costs with coverage.

What is needed is a secure, portable electronic record of an individual's past and present health history. An electronic device, such as a smart card's microcontroller chip, can serve as a patient's healthcare passport, containing vital medical information and linking to other health information. A healthcare smart card can provide efficient information access to all healthcare providers involved in the treatment of a patient.

As chip technology improves and memory integrated circuits become smaller, it becomes more and more feasible to store a substantial subset of a patient's medical record on a single smart card, making it a health record of convenience. However, prior to establishing a portable health record, decisions need to be made regarding the type of information to be stored, how data is actually stored on the card, and the interface used to transfer data between other systems.

In the recent past, smart card-based record management consisted of the storage of limited medical records on smart cards using codification schemes. Even as the memory in smart cards has increased, the amount of patient medical data to be accessed had outstripped the storage capacity of most smart cards. Further, with improvements in Internet security, there has been some movement in medical record management toward storing less medical data directly on the card, and relying on the storage of pointers on the smart card that provides online access to remote information. These pointers can access complete medical record files stored within a specific healthcare network or in national healthcare repositories. With the recent announcement by microchip manufacturers that smart cards can support 1-4 Mbytes of flash memory, there is now more discussion about storing everything from emergency medical information to medical histories, ongoing treatments, and laboratory results – all on a smart card.

In spite of these advances in memory capacities, or perhaps because of them, there appears to be a significant divergence of opinion about whether the smart card should be used as a secure mobile repository of substantial health data or as a secure token to access or point to distributed repositories of patient health or insurance data. There appears to be a solid business case for both; and it seems prudent for many enterprises to consider a combination solution: placing critical health information such as emergency and insurance eligibility data on the chip, while providing access to the appropriate databases for additional records. Regardless of the type of information to be stored, smart card technology offers the flexibility to accommodate an ever growing array of healthcare-related applications. The key to unlocking that flexibility is adherence to standards.

Two standards in the United States currently support portability of medical records: the HL7 standard and the CCR standard.

2.2.1 HL7 Standard[1]

Health Level Seven (HL7) is an American National Standards Institute (ANSI)-approved standards development organization. HL7 develops a variety of standards (sometimes referred to as specifications or protocols), the most widely used being a messaging standard that enables different healthcare applications to exchange key clinical and administrative data.

Currently, most healthcare standards-development efforts focus on the requirements of a particular department. HL7's effort is unique, in that it focuses on the interface requirements of the entire healthcare organization. HL7 also develops standards that are both responsive and responsible to its members as quickly as possible. The group addresses the unique requirements of installed hospital and departmental systems, some of which use mature technologies.

[1] HL7 Web site, http://www.hl7.org/

While HL7 focuses on addressing immediate needs, the group also dedicates effort to ensuring concurrence with other U.S. and international standards-development activities. In addition, HL7 strives to identify and support the diverse requirements of users, vendors, and consultants alike.

HL7 recently announced a joint effort with ASTM International to provide implementation guidelines based on using HL7 protocols for ASTM's continuity-of-care records (CCR) standard (described in Section 2.2.2, below).

2.2.2 CCR Standard and ASTM International

The continuity-of-care records (CCR)[2] standard was defined by ASTM International[3] and a number of health-related associations. The standard was the response to a need to organize and make transportable the most relevant and timely facts about a patient's condition. It is intended to improve and foster continuity of care, reduce medical errors, strengthen patients' roles in managing their health, and assure at least a minimum standard of secure transportability for health information.

Using standards will provide for a consistent transfer of health record information among providers which can also be linked to the HL7 and/or the Clinical Document Architecture (CDA) of most hospitals and their physician practices. The HL7 CDA (known earlier as the Patient Record Architecture (PRA)) is an XML-based document markup standard that specifies the structure and semantics of clinical documents for the purpose of exchange. CDA "provides an exchange model for clinical documents such as discharge summaries and progress notes, and brings the healthcare industry closer to the realization of an electronic medical record. By leveraging the use of XML, the HL7 Reference Information Model (RIM) and coded vocabularies, the CDA makes documents both machine-readable (so they are easily parsed and processed electronically) and human-readable so they can be easily retrieved and used by the people who need them. CDA documents can be displayed using XML-aware Web browsers or wireless applications such as cell phones."[4]

Implementing these recognized data standards (CCR and HL7), and leveraging already existing infrastructure will increase the return on investment of legacy systems while offering inexpensive and secure access to vital data.

Additional information about the types of information that can be included in a portable medical record can be found in Appendix III.

2.3 Reducing Administrative Costs

Healthcare in the United States is subject to ever-increasing financial pressure. Patients are increasingly responsible for fees, the public demand for cost-effective care is growing, and the payments provided by government and commercial insurers are shrinking—all at a time when 48 million Americans are uninsured. And healthcare providers still suffer from the difficulties associated with managing the revenue cycle and reducing write-offs due to bad debt. Patient fees left uncollected due to bad address information, human error, or operational inefficiencies eat away at the bottom line, and significant debt is often never recovered. In addition, bad debt write-offs, which historically were considered a necessary cost of business, continue to increase. According to a recent article in *Healthcare Financial Management*[5], one provider organization's

---

[2] The CCR was developed by ASTM Committee E31 on Healthcare Informatics, Subcommittee E31.28 on Electronic Health Records. The standard defines a core dataset of the most relevant and timely facts about a patient's condition. For maximum utility, the CCR should be prepared in a structured electronic format that is interchangeable with electronic health record systems. For additional information, see http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/REDLINE_PAGES/E2369.htm?L+mystore+wqln2470.

[3] ASTM Web site, http://www.astm.org

[4] "Health Level Seven to Release First XML-based Standard for Healthcare," http://www.hi-europe.co.uk/files/2000/9976.htm

[5] *Healthcare Financial Management*, Volume II, Issue 10, Healthcare Financial Management Association, 2003

bad debt rose 22.5 percent from 2001 to 2002, after a 30.6 percent increase over the previous 3 years.

The American Hospital Association commissioned PriceWaterhouseCoopers to conduct a nationwide study of the paperwork and documentation demands in healthcare.[6] The study produced the following results:

1. In the emergency department, every hour of patient care requires one hour of paperwork.
2. For surgery and inpatient care, every hour of patient care generates 36 minutes of paperwork.
3. For skilled nursing facility care, every hour of patient care results in 30 minutes of paperwork.
4. For home healthcare, every hour of patient care generates 48 minutes of paperwork.
5. A Medicare patient arriving at the emergency department is required to review and sign eight different forms – for Medicare alone.
6. Hospital staff must complete a 30-item Medicare Secondary Payer questionnaire every time a Medicare patient comes to the hospital whether for inpatient or outpatient care.

Organizations leveraging smart card technology to collect and maintain patient data can experience a significantly higher return on investment, realize improvements in the quality of care, and lower staff costs. Through the use of smart cards and the secure data storage capabilities available with the technology, commonly required data can be retrieved and used to streamline paperwork and reporting requirements. The provider, payer, and retail segments of the healthcare market can all capture and realize improved returns through the use of smart cards.

2.3.1 Improving the Registration and Admissions Process

The registration and admissions process is where many of the mistakes occur that contribute to spiraling administrative costs in U.S. healthcare. The challenge is to make the current process more effective, eliminating duplicate patient records and reducing the time, effort, and expense involved while still ensuring that patient data is properly recorded and linked.

The current inpatient registration process typically requires the following:

1. Upon arrival, the patient must present certain information:

   - All current health insurance information, including an insurance card
   - Physician orders and prescriptions for any tests
   - Referrals from a primary care physician if required by the insurance carrier

   If the patient is scheduled for surgery or is arriving for inpatient services, the patient must be prepared to make decisions about living will/durable power of attorney options. The patient must also be prepared to make partial payment and/or discuss financial arrangements when the co-payment and deductible expenses are due.

2. Upon registration, representatives need a copy of the doctor's orders indicating whether the patient is an outpatient, inpatient, or there for observation.

3. To support a patient's admission to the hospital, even as an outpatient, registration requires personal and demographic information, insurance information, and appropriate signatures.

   The admissions process can take anywhere from one to two hours depending on how many tests are ordered by the physicians. If tests have been performed at the doctor's office, the doctor's office must have the results faxed to the pre-admission testing area.

4. On the day of a procedure, patients must typically arrive approximately 1.5 hours before the procedure.

The current outpatient registration process typically requires the following:

[6] "Patients or Paperwork? The Regulatory Burden Facing America's Hospitals," American Hospital Association, 2001, http://www.pwchealth.com/cgi-local/hcregister.cgi?link=pdf/ahapaperwork.pdf

1. The patient must sign in at the central registration desk.
2. A registrar must verify that the patient's information is current and process the order for outpatient services.
3. The patient must be directed to the appropriate destination.

2.3.2 Problems Inherent in Registration and Admissions

The current registration process suffers from several problems:

- The registrar in the healthcare provider's facility must perform a variety of activities – selecting correct forms, copying insurance cards, producing a wristband, and notifying the appropriate areas of the facility of the expected care path for the patient.
- Patient identification on registration documents may depend on whether the embosser equipment is working properly.
- Staff must notify physicians and payers of an admission and carry documents throughout the facility. Critical forms and steps to protect the revenue stream are often overlooked.

All in all, the typical registration process is inefficient and expensive, and more importantly, does not lead to a satisfying experience for most patients or facility staffs.

2.3.3 Improving Registration and Admissions with Smart Cards

Table 1 itemizes the problems that can occur as a result of the current registration process and indicates the benefits achievable using smart cards and related technologies.

Table 1. Registration Process Problems, Solutions, and Benefits

Problem	Solution	Benefit
Caregivers and patients experience lengthy delays.	Smart cards can be combined with a registration kiosk. Data from the smart card can be verified with an easy-to-use touch screen interface. Caregivers can add data to the smart card as they provide care. Centralized patient information can be compared to smart card information, ensuring that the most recent data is available. Primary care providers can use the rapid registration queue to provide patient status information, respond quickly, and complete patient transfers or discharges.	Results are accessed faster; delays are cut by 2/3. Paper-based registration is eliminated. Updating data as a separate task is eliminated. Patient delay in the registration process is minimized. Documents and information, including insurance, are validated using the smart card. Patients spend less time in the discharge/transfer process.
Treatments, medication, or requests for information are duplicated.	A single patient treatment summary can be provided.	Duplicate treatment orders or information requests are eliminated. Treatment errors are reduced. Risk of overmedicating or mis-medicating the patient is lowered. Payers can reduce costs caused by duplicate claims.

Problem	Solution	Benefit
Patient information is incomplete or inaccurate.	Data can be validated as it is entered. A single patient treatment summary can be provided. Patient information critical to admissions (e.g., contact information, demographics, insurance providers, allergies, medications, living will, power of attorney) can be stored on a smart card.	Data validation prevents incomplete entries. Single treatment summaries reduce the risk of inappropriate care. Information about previous patient visits is available when a patient is re-admitted. Insurance plan and other required information is available, resulting in payer savings in call center fees to check patient eligibility Easy availability of patient information speeds the registration and admissions process for both new and returning patients.
Access to patient records is not controlled.	Access to a patient's clinical and administrative records can be role-based and authenticated by the smart card and biometric data.	Need-to-know access to all patient-related information based on caregiver role enforces hospital and regulatory policies.
Colleagues cannot be notified easily of test results or a change in patient status.	Smart cards combined with a rapid registration kiosk can provide a centralized location for patient status. Automatic notification can be implemented.	Caregivers can respond more quickly. Patients experience less waiting time.
Audit trails are lacking.	Each step in the process can be time-stamped using the combination of a smart card and biometric data.	Audit trails facilitate more accurate resource planning and staffing.

2.3.4 Results

Any improved process must start with codified data that is validated by external sources and that is supported by a secure smart card. By streamlining the pre-registration and registration processes and implementing new, more accurate database search techniques, registration staff can identify patients quickly and correctly. More rapid and accurate identification reduces the cost of claims for both the payer and the provider. The provider benefits because the claim is codified and "clean" before it leaves the provider's organization. The payer verifies eligibility more quickly, without the requirement for telephone follow-up. In addition, payers spend less time adjudicating received claims, since the received claims are "clean."

A number of benefits are realized by using smart cards.

1. The entire registration process can be automated and customized, based on the services offered and needs of each patient.

   Automation significantly reduces the time and staff required to complete patient registration, therefore reducing patient wait times. Patient information commonly used for admissions is stored on a smart card thereby reducing the amount of time required to register. By reducing the amount of redundant patient information captured in the pre-registration and admissions processes, accuracy is improved and the amount of paperwork and time in the registration process is significantly reduced – by an order of magnitude – resulting in lower costs and improvement in the patient experience. The downstream effect of more timely and accurate patient data also reduces the number of claim denials by increasing the accuracy of billing information.

2. Workflow is optimized, as admissions personnel no longer have to access multiple machines and multiple information systems to compile registration information.

Personnel simply read the smart card information and validate it in one simple step. Smart card software can validate all information provided by the multiple sources and can register the patient.

3. The registration process is significantly more efficient and is standardized across all healthcare system facilities, leading to operating efficiencies throughout the healthcare network. The downstream revenue cycle improves for payers as well as connected healthcare facilities such as physician offices, pharmacies, schools, and universities.
4. Doctors and healthcare professionals have higher levels of satisfaction.
    - They are able to spend more time on patient care and less time on documentation. In 2002, 40 cents of every healthcare dollar were spent on administrative and paperwork tasks[7] – activities that a smart card can significantly reduce by providing secure access to accurate information at every step in the process.
    - Accurate, usable information is communicated in a timely manner; diagnosis and treatment can begin more quickly.
5. Patient services improve, as more patient-centric information is captured and communicated through the smart card network and applications.
6. Smart cards combined with rapid registration lead to an overall reduction in errors and to communication of more accurate and timely information between all healthcare segments.
7. Health information distribution is simplified. Instead of being hand-delivered, forms are distributed electronically and securely to remote locations.
8. Liability risks are mitigated. All key information that must be communicated to patients by law is automatically provided by the smart card and included in the patient registration process.

2.4 Reducing Healthcare Fraud

Healthcare fraud can affect everyone. Although only a small percentage of healthcare providers and consumers deliberately engage in healthcare fraud, even a modest fraud level can raise the cost of healthcare for everyone.

2.4.1 What is Healthcare Fraud?

Healthcare fraud is committed when a dishonest provider or consumer intentionally submits, or causes someone else to submit, false or misleading information for use in determining an amount of payable healthcare benefits.

Examples of provider healthcare fraud include the following:

- Billing for services not actually performed
- Falsifying a patient's diagnosis to justify tests, surgeries, or other procedures that are not medically necessary
- Misrepresenting procedures performed to obtain payment for non-covered services, such as cosmetic surgery
- Up-coding, or billing for a more costly service than the one actually performed
- Unbundling, or billing each stage of a procedure as if it were a separate procedure
- Billing a patient more than the co-pay amount for services that were prepaid or paid in full by the benefit plan under the terms of a managed care contract

[7] Lane, Sara Gunther; Longstreth, Elizabeth; Nixon, Victoria; *A Community Leader's Guide to Hospital Finance*, The Access Project, 2001, available at http://www.accessproject.org/downloads/Hospital_Finance.pdf

Examples of consumer healthcare fraud include the following:

- Filing claims for services or medications not received
- Forging or altering bills or receipts
- Using someone else's coverage or insurance card

2.4.2 Estimated Costs of Healthcare Fraud

According to the National Health Care Anti-Fraud Association, nearly $85 billion was lost to healthcare fraud nationwide in 2003.[8] That figure is 5 percent of the $1.7 trillion spent on healthcare nationwide in that year. Blue Cross and Blue Shield reported recovering $240 million in 2003 by fighting fraudulent claims, a 52% increase over 2002.

According to Byron Hollis, anti-fraud director for the trade association of the Blue Cross and Blue Shield insurance plans, "Every dollar stolen from the healthcare delivery system by fraud perpetrators is a dollar not available for necessary life-saving treatments, drugs, research or emergency services."[9]

2.4.3 Combating Healthcare Fraud

As an example, consider Medicaid and prescription fraud.

Medicaid is the largest source of funding for medical and health-related services for people with limited income. The average number of Medicaid enrollees in 2003 was estimated to be about 41.9 million, the largest group being children (19.3 million or 46 percent). In 2001, 12.5 percent of the U.S. population was enrolled in the Medicaid program.

More than 46 million people received healthcare services through the Medicaid program in FY 2001 (the last year for which beneficiary data are available). In FY 2003, total outlays for the Medicaid program (federal and states) were $278.3 billion,

Given the magnitude of the actual funds involved in Medicaid, it is understandable why this system is rife with fraud. The effort to combat fraud with smart cards has had mixed results, but the technology still holds great promise to potentially save billions of dollars. Early programs using smart cards as part of a solution to combat fraud failed or performed marginally for various reasons. In many cases, the lack of understanding of how to apply the technology was the key to the poor performance. Some state-based smart card fraud prevention programs were initially funded in pilot, but were never rolled out in full implementation.

In the past several years, states such as Texas, Tennessee, Kentucky and California have all attempted smart card programs addressing different facets of Medicaid and Medicare fraud. The Texas Medical Integrity Project (described in Section 6.4) is one example that illustrates how smart card technology can help to reduce both intentional and unintentional healthcare fraud.

This section provides another example – prescription fraud – and discusses how smart cards can be effective at mitigating the risk of fraud in this area of healthcare.

"The vast majority of healthcare providers want to do the right thing," said CMS Administrator Mark B. McClellan, M.D., Ph.D.[10] Without the ability to audit prescription transactions, the providers and patients will be the ones who suffer the most.

---

[8] "Medical-claims fraud tough to control," MarketWatch, July 13, 2004, http://www.marketwatch.com/news/story.asp?guid=%7B2BA7CB94-97A6-4A2A-BB5D-96B2AC6E939B%7D&siteid=google&dist=google

[9] "Health Insurance Fraud Account for 5% of U.S. Healthcare Expenditures in 2003, Report Finds," California Healthline, July 14, 2004, http://www.californiahealthline.org/index.cfm?Action=dspItem&itemID=105595&ClassCD=CL103

[10] "CMS Strengthens Efforts to Reduce Fraud and Abuse in Medicare, Medicaid," CMS press release, August 27, 2004

A smart card-based prescription auditing program can use both online and offline modes of operation. A simple PC/SC smart card reader/writer is installed using a USB port on the computer in the physicians' offices that provide Medicaid and Medicare services. The computers run a simple application that enables the physician prescribing medications to do so by "burning" those prescriptions on the smart card. Card readers must also be installed in the pharmacies accepting smart card-based Medicaid and Medicare prescriptions.

When a patient in the public health system receives a prescription, that prescription is securely written to the smart card. The patient then takes that smart card to a participating pharmacy and the smart card provides the prescription detail to the pharmacists. Once the prescription has been filled, the smart card is updated so that the prescription history is maintained, but the current prescription for a specific drug is locked and cannot be filled again. If the pharmacy or physician office is online or connected to the central state system, a secure message is sent to the central database and an audit trail is created for that patient, physician and pharmacist. If the physician or pharmacist system is offline, the smart card maintains the data until the next time the card is engaged by an online system. Because most Medicaid programs require that the beneficiaries be seen once a month to review eligibility, chances are that most data collected in the central data repository will age no more than 30 days. Most pharmacies today, chain or private, have online systems to check insurance eligibility and clinical implications of drug-to-drug interactions. As a result, in this example, the audit will be closer to real-time.

By leveraging smart card technology in this way, many individuals uncovered by any type of health insurance today could be offered coverage from just the savings the smart card provides in the prescription fraud segment.

2.5 Providing Emergency Medical Information

Emergency personnel need to know immediately about patient medical conditions and allergies. Storing critical emergency data is an important application for smart cards. Information such as a patient's blood type, allergies, and medications can be stored in a standard and easily accessible format for transmission to a waiting emergency department staff. On many occasions, patients requiring care are unconscious and cannot speak for themselves. Elderly patients may not recall the names of medications that they are taking. Patients may speak a different language and be unable to communicate with doctors or other emergency personnel. A smart card with emergency medical information enables individuals to transport their data to multiple healthcare facilities and provides emergency medical personnel with instant and secure access to access vital medical information.

Healthcare organizations nationally are adopting the American Health Information Management Association (AHIMA)[11] health summary, which is formatted to store and report critical information efficiently. An AHIMA-based emergency health summary includes the following information:

- Patient identification and summarized demographics
- Blood type
- Allergies
- Medications
- Conditions/treatments

Other information that can be included with emergency medical information includes advanced directives (e.g., living will), insurance information, religious preference and emergency contact information.

Emergency personnel can use a portable reader that securely accesses the information stored on the smart card's chip. The patient's previously recorded medical history can then be viewed on a

[11] AHIMA (http://www.ahima.org) is the premier association of health information management (HIM) professionals. Founded in 1928 to improve the quality of medical records, AHIMA is committed to advancing the HIM profession in an increasingly electronic and global environment.

computer screen. The emergency healthcare professional then has immediate access to the patient's medical history, and can thereby provide better care.

As an example, consider a routine exam in which a physician diagnoses a patient with Type II diabetes. If the patient has a smart card that stores critical medical information, the physician adds the new diagnosis with treatment plan. The next time the patient's card is used, it provides the healthcare professional with the Type II diabetes diagnosis, treatment plan and name of the physician who entered the information.

The lack of medical information can result in tragic results, where professionals make the correct decisions – by the book and by judgment – but fail to save the patient. Two examples follow.[12]

- In 1997, a 42-year-old man who was born with hepatitis C and who had been on medication for the condition was involved in an automobile accident. There were no life-threatening injuries. The emergency medical technicians (EMTs) secured all vital signs and, while in transit, were in communication with the emergency room (ER) physician and staff at the assigned medical facility. The patient was suffering neck and back pain during standard transportation. The ER staff recommended administering Tylenol III, which cannot be used by hepatitis C patients. The patient died en route less than five minutes after receiving the Tylenol III. Neither attending EMTs nor ER staff could reverse or diagnose the condition or situation.
- An elderly lady was 81, alert, and cheerful. However, she appeared to be overly-medicated. Concerned friends reviewed her medications and discovered that she had 41 prescriptions! Four bottles were vitamins, minerals, and calcium. One drug was prescribed in seven different, but similar, medications. The total dosage was at an overdose level when taken as prescribed. Fourteen medications were eliminated when the five prescribing physicians were informed of the duplications.

Situations such as these are not unusual. When healthcare professionals need answers to medical questions, the data are not always available. They are taking risks trying to save lives while waiting for critical information. Making emergency medical information available on a secure portable smart card may decrease the number of tragic and needless deaths that result from the lack of critical information when it is needed most.

The Florida eLife-Card program (described in Section 6.4) illustrates how smart cards can be used to provide emergency medical information.

2.6 Strengthening Patient Loyalty

Loyalty marketing (also called customer relationship management or one-on-one marketing) is a powerful tool for retaining valuable customers, building market share, and enhancing profits. Cultivating customers who are committed to one's brand is a huge marketing advantage.

The concept of loyalty marketing is thriving in healthcare markets. Most successful healthcare loyalty programs have one or more of the following objectives:

- Increase patient acquisition and retention
- Increase brand recognition
- Increase the enterprise's knowledge of the patient base
- Increase patient knowledge of and loyalty to the healthcare enterprise

Healthcare loyalty programs using smart cards can dramatically improve the value of the smart card and differentiate the brand to the cardholder. Smart card-based solutions have key advantages over magnetic stripe or paper-based loyalty programs, by providing:

- The ability to store extensive demographic and medical information

[12] *Source:* Orlando Regional Medical Center

- The ability to update patient data (e.g., diagnoses and treatments) instantly
- Stronger security
- Support for multiple healthcare applications on one card

2.6.1 Increase Patient Acquisition

Industry statistics indicate that it is much more costly to acquire a new patient than to retain an existing one. Many healthcare loyalty programs therefore focus on both attracting and retaining new patients.

Loyalty programs are designed to modify patient attitudes toward a hospital or other medical enterprise. Thus, a hospital might streamline the check-in process, provide patients with a card listing emergency medical information, offer special wellness services, facilitate doctor referrals, or simply provide patients with a private and secure means of obtaining information about their own medical records. Smart card-based loyalty programs enable healthcare enterprises to recognize patients immediately at registration, thereby enhancing patient convenience, enabling self check-in (which in turn can lead to lower enterprise costs), reducing the incidence of duplicate patient records, and providing immediate written confirmation to the patient (for example, by printing out the day's itinerary or a map of where the patient is to go).

Healthcare enterprises are also driven to reduce operating costs. One way to reduce costs is to switch from mass-marketing approaches to targeted initiatives that attract patients to specific services. A smart card-based loyalty program is ideal for informing patients about special services or encouraging participation in specific initiatives by displaying promotional messages to the cardholder when the card is inserted in a kiosk.

2.6.2 Increase Brand Recognition

The U.S. healthcare system is fragmented. Healthcare has therefore become increasingly competitive, lowering profit margins. Loyalty programs help differentiate services and build brand awareness in the community. Building brand awareness is a key goal of most healthcare enterprises.

2.6.3 Increase Knowledge of the Patient Base

Loyalty marketing for commercial requirements can be used to build a reservoir of valuable data about patients. A loyalty program gathers data describing patient demographics, frequency of visits, and patient needs. That knowledge increases the effectiveness of advertising and promotional activities and improves healthcare programs at all patient points of contact.

The ability of smart cards to disaggregate data and encrypt information protects the individual's right to privacy while creating a confidential and efficient method of sharing patient information between healthcare facilities. Smart cards support the transfer of important health information and interface with the health information system's billing and collection functions. Thus, smart cards can also play a key role in areas such as clinical research. Provisions for confidentiality can make patients less reluctant to reveal, and physicians and researchers more eager to record, accurate information that can be used for research.

2.6.4 Increase Patient Knowledge

Traditionally, patients have lacked control over the health records maintained for them at healthcare facilities. However, patients are becoming more savvy about what they need to do to sustain wellness and when to obtain treatment. They are demanding access to their medical information while insisting on security and privacy for that same information.

Smart cards are among the few electronic devices that can enhance privacy and authentication. Unauthorized people can neither read what is stored in the smart card chip nor use the card to access records stored remotely. Smart cards also interact reliably with a wide range of systems. They can operate over the Internet to verify information in a carrier's database, and they can be read and updated offline at a physician's office, as medical clerks prepare electronic claims for

submission to an insurer. Patient information on the card can be updated immediately, and the patient can print out what is stored on the card.

Knowing that the card can unlock critical personal information is often an incentive to be a member of a particular loyalty program. A dynamic offering at the point of service based on a patient's personal information, such as a discount on drugs or enrollment in a special program, can also affect a patient's experience positively. For example, the use of personalized information to suggest targeted wellness programs can significantly increase a patient's connection to the healthcare enterprise.

2.7 Complying with Government Initiatives and Mandates

Data protection is a key concern for any information system. Healthcare smart cards secure cardholder information, verify cardholder eligibility, and protect data – features that are critical to ensuring that healthcare providers, insurers, and patients have necessary information that is relevant to their specific requirements. Smart cards facilitate secure health insurance administration and are both flexible and portable, thereby accommodating mobile populations and dynamic healthcare programs. A typical healthcare smart card can contain (or provide remote access to) a detailed profile of the cardholder, including the individual's coverage, deductibles, and any co-payment, pre-authorization, or referral requirements. Graduated access rights allow issuance authorities and authorized individuals to update information at the point of care, ensuring that data are accurate and reliable. Security features resident on the card prevent unauthorized data modification and tampering. Risk management rules stored on the card when the card is personalized can be modified when the card is connected remotely to the issuer system.

2.7.1 Federal Privacy Requirements

For healthcare information systems, concerns about data security are heightened by HIPAA, the Federal legislation that mandates increased security for patient health data storage and access. HIPAA strongly encourages electronic data transactions and requires that electronically-stored healthcare information be kept private and secure. HIPAA applies to health plans, healthcare clearing houses, healthcare providers, hospitals, medical groups, and physicians.

2.7.2 Public Health Programs

Public health programs, including government programs such as Veterans Administration (VA) health services, Medicaid, Medicare, food stamps, Head Start, immunization services, the Childhood Lead Poisoning Prevention Program, the Special Supplemental Nutrition Program for Women, Infants and Children (WIC), the Commodity Supplemental Food Program (CSFP), and the Farmers' Market Nutritional Program (FMNP), all focus on collecting and accessing demographic, anthropometric, nutritional, and medical information about members of a household to provide for their healthcare needs.

In the United States, most public health initiatives are federally funded but state operated. These programs tend to support both electronic benefits transfer (EBT) and electronic services delivery (ESD) systems. The information needed for EBT and ESD programs can be consolidated on one smart card, eliminating the need to reenter demographic and personal data from program to program. The portability and security of the healthcare information significantly increases participant convenience. Another advantage of this approach is that it offers the potential for sharing information and reducing paperwork. Maintaining shared records on the chip of a government-issued smart card improves case management: appointments are coordinated more easily and referral tracking is improved.

The Health Passport Project (HPP) is one example of ESD at work. HPP is an initiative of the Western Governor's Association. Over the past several years, the HPP has tested and evaluated the use of smart cards to integrate health data and deliver benefits across a range of government programs administered by different agencies. The HPP places client healthcare records on a smart card. When clients seek services from more than one program, their health information is

read from the smart card and transferred to the new provider's system. Consequently, there are fewer gaps in information and less duplication, and less time is spent by both the patient and the healthcare providers processing paperwork or scrambling to locate more up-to-date information about issues such as a child's allergies or immunization records. The new provider then adds the updated information to the smart card health record.

In cooperation with the General Services Administration, the Department of Defense, and California WIC, the HPP designed a Web-based virtual patient account (VPA) to test the impact that ready access to health information would have on the delivery of WIC benefits to participants at the U.S. Marine Corps base at Camp Pendleton, CA. The Camp Pendleton Health Center enters health data directly into VPAs for WIC participants before referring them to the WIC clinic. The Health Center staff adds, updates, or reviews the medical data in the VPA when providing care, as aligned with HIPAA guidelines.

In the Camp Pendleton pilot (currently underway), smart cards are issued to military dependents who participate in WIC. In addition to the WIC EBT application, the card carries the VPA application, which makes the cardholder's health data accessible to WIC via a secure Web site. The patient information stored in the VPA can be accessed securely through a Web-browser, potentially making the information accessible to multiple legacy applications. The card carries a digital certificate that authenticates the identity of a participant or healthcare provider, common demographic information used across programs, and information about the programs in which the cardholder participates. Providers are also issued HPP cards that contain the digital certificates required to authenticate their identities and access participant data.

2.8 Supporting Multiple Applications in Healthcare

As a portable data platform, a smart card has utility beyond medical applications. Smart card applications can automate and streamline almost every touch-point in a healthcare enterprise. A single smart card can carry multiple applications, including both contact and contactless applications. The card can even contain a magnetic stripe or bar code, if required.

Our pockets and purses are crammed full with an assortment of single purpose cards and keys. Each performs a separate function. Smart cards provide an alternative, combining a variety of applications not normally associated with healthcare. With its offline portability, smart cards promote self-service, help improve customer convenience, trigger customized services, and create a mechanism to deliver new products and services. Smart cards function as electronic sentinels to protect data, property and networks. They are identity badges with access privileges. They track assets and provide privacy safeguards. They reduce paperwork and streamline controls. Most importantly, smart cards serve as an information platform that can support an array of applications not even conceived a decade ago.

Table 2 presents some additional candidate applications for a healthcare smart card.

Table 2. Applications for a Multi-application Smart Healthcare Card

Application	Use
Physical access	Location access: a campus, a building Building interior access: entrances, lobbies, offices, computer rooms, vaults, intensive care or disease confinement areas Credentialing for employees and vendors Time and attendance for employees
Logical access	Network access: LANs, WANs, signed and encrypted e-mail, secure transactions Human resource benefits Laboratory specimen results Secure physician conferences regarding specific patients

Application	Use
Data storage for individuals or families	Organ donation information Loyalty data Health insurance information, including co-pays and insurance coverage Pharmacy prescriptions, doctors orders Tracking medical equipment usage (e.g., rehab machines or CAT scans)
Financial	Electronic purse: cafeterias, gift shops, vending machines, parking. Healthcare prepayment accounts to support co-pays and similar payments

3 Conclusions

The healthcare market is on the cusp of a move from physical paper to an electronic world. In the era of managed care, specialized medicine, thin financial margins, identity fraud, insurance claims submission hassles, and government demand for secure, portable and confidential patient information, the competitiveness of healthcare providers depends on the proper use of information technology. Increased computerization, database use, and movement of sensitive patient information require focused controls on maintaining the security and confidentiality of those records.

As the industry advances electronically, it must provide heightened records security and ensure confidentiality of individually identifiable patient information. Data protection is the key concern, fueled by legislation such as HIPAA to increase security of patient health data storage and access. The mobile nature of today's healthcare administration requires immediate and secure information access without compromising privacy. This presents smart card technology with a unique opportunity to provide solutions that encompass secure information access and management, while supporting data mobility and maintaining privacy.

Healthcare administrators are major consumers of paper and ink. Patient records, medical claim forms, clinic referrals, prescriptions, and appointment booking systems remain manual processes at most healthcare enterprises. Those few areas that are automated tend to operate as independent silos. Industry sources point out that only a minority of physician practices have patient data stored in an electronic format. Physicians and other healthcare professionals have developed a stubborn affinity for file folders and other paper-based mediums for collecting and retaining patient data. In driving healthcare professionals to expend more time and effort with patients and less with paper files, the healthcare industry will require substantial employee re-training efforts as well as a significant technology investment.

Smart cards help reduce healthcare paperwork and secure access to patient records and health insurance status. The smart card is an ideal medium for holding encrypted patient information, and for computing a digital signature or a biometric template to reduce ambiguity about the cardholder's identity. Fraud reduction in health benefits also favors smart card implementation, and it remains a significant issue for government. HIPAA is technology-independent and does not specify the use of smart cards or any other technology. However, it is likely many healthcare enterprises will choose smart card technology due to its suitability for secure data handling and fraud reduction.

There also exist many opportunities with healthcare insurance. Paper-based eligibility verification and claims processing are too often characterized by redundant information collection, lengthy waits, and multiple forms needed for reimbursement. The manual processes used increase the risk of transposition errors. The inefficiencies of traditional eligibility verification and claims processing cost insurers, national health agencies, and healthcare providers significant amounts of time, resources, and money. Too often, they result in significant delays for referrals, treatment and reimbursement for the insured patients.

Smart cards can provide clean data for eligibility verification and claims processing. They not only prevent administrative errors and streamline payments, but they also prevent medical errors that can arise when one practitioner doesn't know what the other has been doing. Test results conducted by one clinic could be available to all practitioners. Before prescribing a drug, the physician would know the patient's recent diagnoses, allergies, prescription history, and any over-the-counter drugs that may conflict with the proposed course of treatment. In the long run, the data carried by smart health cards can not only prevent illness and save lives, but can also save the healthcare industry billions of dollars.

Today, many patients lack control over their health records maintained at clinics, pharmacies and hospitals. However, with smart card technology, no one can read what is contained on the smart card's microchip, or have access to computerized records without one's personal identification number (PIN) and authorized hardware and software. Smart cards are among the few electronic devices that are privacy-enhancing. Further, they interact reliably with a wide range of systems.

They can operate over the Internet to verify information in a carrier's database, and they can be read and updated offline at a physician's office, as medical clerks prepare electronic claims for submission to the insurer.

Moreover, the ability of smart cards to disaggregate data and to encrypt information protects an individual's right to privacy while creating a more efficient method to share patient information from one healthcare facility to another. Smart cards transfer important health information, and participate in the health information system's billing and collection functions. Thus, smart cards can play a key role in areas such as clinical research. With provisions for confidentiality, patients seem less reluctant to reveal, and physicians and researchers are more eager to record, accurate information for research.

Whether the smart card carries critical medical data and clinical information, or evolves as a secure key to distributed repositories of patient information, or a combination of both, it is a technology whose time has come. Smart cards are a practical enabling technology to enhance the privacy and confidentiality of patient information. Further, they are intuitively easy to use; indeed, they can even be rendered "dummy proof."

This paper has discussed some of the daunting challenges facing the U.S. healthcare industry today and has identified clear opportunities for the employment of smart card technology to address and resolve these issues. In recent years, there has been a pronounced effort to establish and refine standards for maintaining and moving healthcare data. With continued advances in smart card technology and the increased awareness of its practical solutions, healthcare organization use of that technology is gathering momentum. This paper has cited some examples of smart card use, and has suggested additional applications for consideration. Of course, there are a plethora of new healthcare applications waiting for discovery and implementation.

4 References and Resources

ASTM International web site, http://www.astm.org

"CMS Strengthens Efforts to Reduce Fraud and Abuse in Medicare, Medicaid," CMS press release, August 27, 2004

A Community Leader's Guide to Hospital Finance, Lane, Sara Gunther; Longstreth, Elizabeth; Nixon, Victoria; The Access Project, 2001, available at http://www.accessproject.org/downloads/Hospital_Finance.pdf

Health and Human Services Commission Request for Proposals for Front End Authentication and Fraud Prevention System Pilot Program, RFP #529-04-085, October 1, 2003

"Health Insurance Fraud Account for 5% of U.S. Healthcare Expenditures in 2003, Report Finds," California Healthline, July 14, 2004, http://www.californiahealthline.org/index.cfm?Action=dspItem&itemID=105595&ClassCD=CL103

"Health Level Seven to Release First XML-based Standard for Healthcare," http://www.hi-europe.co.uk/files/2000/9976.htm

Healthcare Financial Management, Volume II, Issue 10, Healthcare Financial Management Association, 2003

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

HL7 web site, http://www.hl7.org/.

Medicaid Integrity Pilot: Independent Evaluation Final Report, International Biometric Group, 2004 (http://www.hhsc.state.tx.us/OIE/MIP/020105_MIP_EvalRpt.pdf)

"Medical-claims fraud tough to control," MarketWatch, July 13, 2004, http://www.marketwatch.com/news/story.asp?guid=%7B2BA7CB94-97A6-4A2A-BB5D-96B2AC6E939B%7D&siteid=google&dist=google

"Patients or Paperwork? The Regulatory Burden Facing America's Hospitals," American Hospital Association, 2001, http://www.pwchealth.com/cgi-local/hcregister.cgi?link=pdf/ahapaperwork.pdf

Smart Card Alliance Healthcare Council, http://www.smartcardalliance.org/about_alliance/councils_hc.cfm

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

5 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Healthcare Council to provide an overview of the value of smart card technology for healthcare applications in the U.S. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Healthcare Council members for their contributions. Council participants involved in the development of this white paper included: ACI Worldwide, Axalto, Booz Allen Hamilton, CardLogix, Competech Smart Card Solutions, EDS, EMIDASI, Gemplus, Giesecke & Devrient, Healthmeans, Hitachi America Ltd., IBM, LEGIC Identsystems, Lockheed Martin, Oberthur Card Systems, OTI America, Smart Commerce, Inc., Sharp, TecSec, Uniliance Health, U.S. Dept. of Defense, VeriFone, Visa USA, Wisconsin Physicians Service Insurance Corporation

Special thanks go to the individuals who wrote, reviewed, edited, and contributed content to this white paper.

- Frank Avignone, Healthmeans
- Jeff Beulke, ACI Worldwide
- Michael Cariou, Oberthur Card Systems
- Paul Davis, Uniliance Health
- Joe Fasulo, EMIDASI
- Bob Gilson, U.S. Dept. of Defense
- Mansour Karimzadeh, Smart Commerce, Inc.
- Mark McGovern, Lockheed Martin
- Cathy Medich, Smart Card Alliance
- William Page, EMIDASI
- Neville Pattinson, Axalto
- John Petty, TecSec
- John Rego, OTI America
- Nigel Smith, Visa USA
- Robert Stuart, Sharp
- Greg Thornton, Competech Smart Card Solutions
- Brenda Washington, VeriFone
- Chuck Wilson, Hitachi America Ltd.

About the Smart Card Alliance Healthcare Council

The Healthcare Council is one of several Smart Card Alliance Technology and Industry Councils, a new type of focused group within the overall structure of the Alliance. These councils have been created to foster increased industry collaboration within a particular industry or market segment and produce tangible results, speeding smart card adoption and industry growth.

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. The Healthcare Council steering committee is led by co-chairs Frank Avignone, Healthmeans, and Paul Davis, Uniliance Health.

Healthcare Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects.

Trademark Notice

6 Appendix I: Implementations Using Smart Cards for Healthcare Applications

6.1 Queens Health Network

The Queens Health Network (QHN) provides over 1 million ambulatory care visits annually to the 2 million residents of Queens, New York. QHN includes two leading acute-care facilities, Elmhurst and Queens Hospital Centers, 15 community-based medical centers and practices, and 6 school-based health centers. The network provides preventive and healthcare services throughout the borough.

QHN began as a means to offer something better to patients. QHN was already paperless, with emergency medical records (EMRs) implemented at the two acute-care facilities, so adopting smart card technology was the next logical step. “We're trying to change our focus to improving health outcomes by moving information better," states Al Marino, QHN’s CIO. "We want to be able to share information not just within our own health system, but within the community, and so patients have access to their information. We're excited about patients being able to provide their information in emergency situations." The card facilitates delivery of care by providing access to patient summary information in an emergency setting, which is especially helpful for patients whose primary language is not English.

Elmhurst Health Connection cards will be issued to about 14,000 patients of the Adult Primary Care service at Elmhurst Hospital. Card issuance is the first step in trying to share more patient information with physicians in the NYC Health and Hospitals Corp., of which QHN is a member, so that smart cards become part of the organization's information infrastructure. Each card carries the patient's photo ID and contains a 64 KByte chip that contains data such as the patient’s name, address, emergency contact, allergies, current medications, and recent lab results. The cards are updated automatically at each patient visit.

The health network has provided free, read-only software and card readers to the emergency rooms at 10 other New York City hospitals. It hopes to work with local hospitals as well as ambulance systems to provide them with software and readers and anticipates providing software and readers to the following organizations:

- Other voluntary hospitals in Queens, including North Shore/Forest Hills
- St Vincent’s Medical Centers
- City ambulances

QHN has spent about $200,000 on the program since July 2002 and hopes to obtain grant money to expand the program to areas such as Women's Health Services.

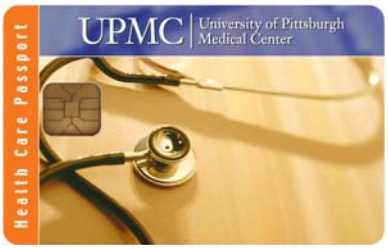
Currently, QHN is collaborating with the other providers in the borough to implement and further develop applications to improve patient safety and the health outcomes of the communities that QHN serves.

6.2 University of Pittsburgh Medical Center

The University of Pittsburgh Medical Center (UPMC) includes19 hospitals and over 5,000 doctors in over 400 offices. In the face of dramatic growth, UPMC faced a challenge: how to ensure that its technology infrastructure kept pace with its business requirements. Processes such as verifying the eligibility of individuals while maintaining the confidentiality of sensitive patient information were critical to the continued success of the organization.

UPMC looked at the smart card as an emerging technology with the potential to enhance administrative processes and system communications. An initiative was undertaken to find a

solution that would then be evaluated to determine whether it enhanced the integration of UPMC's many systems and practices. The objectives for this system were to solve the challenges of complying with data privacy and confidentiality legislation (i.e., HIPAA), enable patients to access and participate in updating their information, and provide a portable solution supporting immediate access and consistent data flow.



UPMC determined that smart cards could play a role in this new system. Following a successful 2-year pilot project, the UPMC smart card, dubbed the Healthcare Passport, has been distributed to 2,000 UPMC patients.

For the patient, the immediate benefits include speeding through the check-in process during office visits. The cards enable better care through faster retrieval of important medical information, according to Scott Gilstrap, Director for Technology Solutions at UPMC. "The smart card eliminates a lot of paperwork for the patient and makes the visit to the doctor more convenient and less stressful," Mr. Gilstrap said. "It can be a true lifesaver, especially for the elderly who may not remember all of the medications they are taking. This information is stored, updated accurately and easily available on the card."

The focus of the smart card deployment so far has been the practice of Solano & Kokales Internal Medical Associates–UPMC. The practice maintains smart card readers for staff to use to access and update patient cards. Patients can use computer kiosks in their physician's office and in examination rooms to access and suggest changes to their medical information in privacy and also to obtain a printed copy of the smart card information. Patients can also purchase a card reader to use with a home computer. Personal identification numbers (PINs) are required to access the data on a card.

With the smart card, patients no longer need to supply their personal information each time they visit the doctor, since the cards contain critical information such as medications, allergies, and chronic conditions. By inserting a patient's card into a computer in the exam room, the physician has instant access to accurate and up-to-date information about the patient.

The UPMC smart card uses sophisticated security measures that make it nearly impossible for strangers or unauthorized personnel to retrieve a patient's medical information. To access information, each patient and physician must have a card and a PIN (two-factor authentication). The cards also may decrease the likelihood of inaccurate billing. About 90 percent of services denied by insurance companies are due to clerical errors made at the time of registration for a clinical service.

Emergency departments equipped with card readers can rapidly access potentially lifesaving information about a patient, such as allergies to medications and chronic medical conditions. The initial rollout included smart card readers at the UPMC Presbyterian Hospital emergency department, the Department of Orthopedic Surgery, the Center for Sports Medicine, and Dr. Solano's practice.

The smart card project is just one component of a progressive information technology initiative at UPMC. The centerpiece of the initiative is the development of an electronic health record to be totally integrated across the entire system, which includes hospitals in both urban and rural settings, hundreds of physician's practices, and nursing, personal care, and long-term care facilities. The goal of UPMC's information technology initiative is to improve the quality of patient care, reduce errors and duplication of services, and be more cost-effective. UPMC believes that information technology affords patients greater access to care and contributes to a more informed, interactive healthcare experience.

6.3 St. Luke's Episcopal Health System, Houston

St. Luke's Hospital was founded by the Episcopal Diocese of Texas in 1954. Located in the heart of the Texas Medical Center in Houston, St. Luke's delivers primary and tertiary healthcare to patients from all over the world. St. Luke's has been recognized as one of the top 10 cardiovascular centers in the United Stated by *U.S. News & World Report,* as well as a magnet hospital for excellence in patient care.

At St. Luke's, medical personnel use networked computers to view patient records stored in a central database. In 2001, St. Luke's instituted a smart card-based system for logging on to the network. The project was initiated to resolve various issues associated with password-based data access. Physicians who worked at different hospitals could not remember their multiple passwords. At St. Luke's, physicians had different logon procedures than nurses. Security was compromised when physicians, in desperation, wrote down their passwords or shared them with staff or residents. These problems also resulted in a flood of calls to the hospital help desk because of forgotten passwords. In addition, doctors needed to access patients' charts and clinical lab results more easily and securely.

The smart card technology, provided by BNX Systems, was implemented for convenience and security. The cards are used simply to provide secure access. Each card is protected by a four-digit PIN. Providing the correct PIN authenticates the doctor to the card; the card then authenticates itself to the hospital's data network, providing two-factor authentication. The card carries only the cardholder's name and a 128-bit key. To log on to the system, a physician simply inserts the card in a reader and types in the PIN.

Initially, 55 out of 250 physician computer stations were equipped to accept the smart cards. St. Luke's installed wall-mounted PCs (at an interval of one per every four rooms) and about 15 desktop PCs and laptops on each floor. All computer stations have smart card readers built into their keyboards.

The two-factor authentication provided by the smart cards improved user access and reinforced data security. Originally, St. Luke's issued smart cards to about 100 of its 1,800 doctors. The program rapidly expanded to include more than 900 physicians. About 450 PCs are now equipped with smart card readers. St. Luke's continues to look for ways in which to connect doctors with data and streamline procedures. The hospital is moving rapidly toward a Web-based portal and single-sign-on capabilities and is considering a variety of other changes. Smart cards led the way in improving physician convenience with regard to patient data access.

6.4 Florida eLife-Card

About 1 million Florida residents carry an eLife-Card smart card issued by EMIDASI [13] for use by emergency personnel: emergency medical technicians, firefighters, police, and personnel in emergency rooms, intensive care units, and trauma centers. The card stores the lifesaving information required for immediate emergency treatment such as information about allergies and current medications and also provides access to expanded information such as religious preferences, living wills, and disclaimers that give medical personnel permission to access the cardholder's records and offer treatment.

In addition to Florida fire departments, emergency medical services, and paramedics, over 15 healthcare organizations in Florida are participating in the program, including hospitals, medical centers, fire and rescue organizations, and life-flight services.

[13] EMIDASI is a provider of card personalization, secure identity solutions, and point of sale transaction services. For more information, see http://www.emidasi.com/.

6.4.1 Background

The eLife-Card smart card was conceived of in 2002, partially in response to emergency healthcare needs resulting from the effects of Florida's hurricanes. People requiring emergency medical care as a result of a hurricane encountered difficulties receiving appropriate care in a timely fashion. Hospitals were not able to locate health records quickly (if the records had even survived); obtaining authority for treatment often involved lengthy delays; and patients often were unable to provide required information.

In 2003, Florida's fire marshals requested assistance in ensuring that marshals injured while helping with hurricane disaster relief would receive emergency care quickly. The marshals then encouraged adoption of the card by the firefighters' union, which in turn suggested that the card be adopted by members of the teachers' union. The card is now also offered by certain hospitals in lieu of (or in addition to) medical alert systems.

The card is not free; unions and most other organizations sell it for $60. One hospital charges $85 per year for the card, but cardholders also receive free parking at the hospital (parking otherwise costs $5 per hour).

6.4.2 Operational Details

The eLife-Card smart card can hold up to 4 Mbytes of data, which includes the following information:

- Personal identification, with or without picture
- Allergies
- Medications
- Medical history
- Emergency contacts
- Advanced directives (living will or Five Wishes)
- Preexisting medical conditions
- Will and probate
- Insurance provider
- Religious preferences
- Doctor visits
- Pharmacy integration, to track prescriptions
- Organ donor status

6.4.3 How the Card Works

The eLife-Card carries both an RFID tag and a smart card chip. Cardholders receive stickers advertising the presence of the card that they place on the back windows of their vehicles and in their glove compartments. Cardholders also receive a plastic key-ring card indicating that they have eLife-Card smart cards.

Emergency responders use an antenna to determine whether a card is present in the area of an accident or other emergency. When a card is detected, responders can see how far away the card is and the direction in which to look for it.

Once the card is located, responders use a handheld personal data assistant (PDA) to read the smart card chip, obtaining information about a cardholder's allergies, medications, next of kin, and primary care physician. This information is typically available within 5 seconds and can then be transmitted to the facility to which the cardholder is being transported. When the cardholder arrives at a healthcare facility, staff can use the card to access a complete health record for the person over the Internet. The card can also interface with over 300 different hospital medical information systems.

6.4.4 Protecting Cardholder Data

The card is HIPAA compliant, and cardholder privacy is protected at all times. The information on the card is encrypted. The PDA used by emergency responders includes a biometric scanner, and responders must provide a fingerprint to authenticate their right to access the information on the card. Healthcare facilities insert the card into a dual-slot card reader. Card information is only accessible after physicians or other authorized personnel have inserted a card in the second slot of the reader.

Cardholders can update personal information over the Internet, using their membership number and a PIN. Healthcare information is updated automatically using health record servers when the card is read at any participating healthcare facility that has Internet access.

6.5 Texas Medicaid

In 1998, the Texas Health and Human Services Commission (HHSC) decided to implement the Medicaid Fraud and Abuse Detection System (MFADS). The MFADS is a key analytical component of the Texas Medicaid Management Information System (MMIS). The number of cases investigated, the dollar amounts identified, and dollar amounts recovered have increased as the result of productivity and efficiency increases generated by the MFADS research tools and ad hoc query-reporting capabilities.

This increased investigative activity and HHSC's consistent enforcement of Medicaid policy and procedures have deterred fraud and abuse in the Medicaid program. At the same time, new schemes, patterns, and trends of fraudulent behavior have arisen. HHSC is continuously working to address these new challenges and continues to believe in exploring new technology to enhance the MMIS.

One of the most consistent fraud patterns involves what are sometimes called "phantom" services—where some providers appear to be billing for services that they are not actually providing. Currently, the only way to identify this type of abuse is to request medical records and confirm the services with the patients, which can be very labor intensive and costly.[14]

HHSC therefore initiated the Medicaid Integrity pilot study, to design and develop a front-end authentication and fraud prevention system. The system had multiple purposes:

- Create a more efficient Medicaid system by reducing the total amount of Medicaid expenditures wasted on fraud and abuse
- Alleviate "phantom billing" within the Medicaid system
- Reduce the amount of fraud associated with provider up-coding
- Prevent client Medicaid ID card sharing and card swapping

6.5.1 How Medicaid Integrity Works

The Medicaid Integrity system works as follows. Clients are automatically issued new Medicaid ID smart cards. At the time of service, the client shows the ID card to the provider. The provider inserts the client's smart card into a point-of-service device to access the data encrypted on the card. The client then places a finger on a biometric scanner. Client identity is validated in less than 1 second. The client then proceeds with normal medical service.

Upon completion of the medical appointment, the client checks out, using the same process and thereby creating a service-visit-duration time stamp. This information is transmitted to the state and ultimately compared to the bill prepared by the provider and submitted to the Medicaid office for payment.

[14] *Health and Human Services Commission Request for Proposals for Front End Authentication and Fraud Prevention System Pilot Program*, RFP #529-04-085, October 1, 2003.

6.5.2 How Medicaid Integrity Helps

Table 3 summarizes how the Medicaid Integrity program supports fraud detection and deterrence.

Table 3. Fraud Detection in the Texas Medicaid Integrity Smart Card Program

Fraud Type	Description	Smart Card Benefit Achieved
Phantom billing	Claim is submitted, but no services were rendered. Client is not even physically present at provider's office.	Verifies client is physically present in the provider location at the time of service.
Up-coding	Provider's claim includes more services than were actually rendered.	Provides time-stamped visit *duration* data. This data is compared to provider billings to identify up-coding fraud.
Card-sharing and ID theft	Ineligible individual uses another's valid Medicaid ID card to receive services.	Verifies entitled client is the only one using the card.

6.5.3 Medicaid Integrity Pilot[15] Description

The Medicaid Integrity pilot study was conducted in six counties. Four vendor teams were responsible for the development, implementation, and operation of the pilot. During the pilot, information was collected to validate the client's presence at the point-of-service, including date, time, and duration of service. This information was compared with traditional Medicaid billing data received by the state.

The initial 9-month pilot involved the voluntary participation of 1,215 Medicaid providers and 228,131 Medicaid recipients and the installation of 954 front-end authentication devices. This level of participation allowed data to be collected from 60,196 client visits and 122,233 transactions. Because the program was not implemented statewide, it is not possible to clearly establish Medicaid fraud reduction from the pilot results. However, biometrics and smart cards were determined to be an effective tool in preventing provider and client fraud within the Medicaid program.

The entire Independent Evaluator Report is available at http://www.hhsc.state.tx.us/OIE/MIP/020105_MIP_EvalRpt.pdf. Further details about the program are available at the HHSC Web site, http://www.hhsc.state.tx.us/OIE/MIP/MIP_Updates.html.

6.6 Sesam Vitale

One of the most successful healthcare smart card projects worldwide is the French Sesame Vitale program. The program, which was started in 1978 and rolled out throughout France between late 1997 and 2001, issues citizens smart cards that are used within the country's health insurance system. When the program was initiated, the French government was the second largest healthcare spender in the world, but citizens were frustrated with the delays encountered in obtaining reimbursement. Reducing administrative costs was the key driver for the project. The government needed to change its approach and develop a more efficient and cost-effective system.

The overall objective of Sesame Vitale was to move from a paper-based healthcare benefits payment system to a system based on electronic transactions. The initial goal was to replace all

[15] *Front End Authentication and Fraud Prevention System Pilot Program Medicaid Integrity Pilot Status Report,* July 1, 2005.

paper bills with electronic care sheets that are transmitted directly by the provider to the insurer. Electronic refunds are assigned to the patient, who only pays a small portion of the bill at the time of service. The program now also enables the electronic transfer of medical records and prescriptions to healthcare agencies responsible for reimbursement. In the previous paper-based system, the French Government took up to 2 months to process claims and reimburse citizens. Today this process typically takes a few days.

The program is managed by the state-controlled social security organization (CNAM). At the onset, doctors and other private practice health professionals were required to install a computer and transmission device in their offices, many of which had no such system at the time. The doctors were then provided with the Sesame Vitale "Health Professional Card." Physicians at first saw the program as government interference in their way of doing business and were reluctant to join. The increased expense incurred by the doctors overshadowed the increases in efficiency touted by the healthcare system. Many patients also did not fully understand the potential benefits. Concerns were also expressed about the potential for invasion of privacy.

After several years, most of these objections are resolved. With the system now in place and running smoothly, information on treatment and cost is processed at the doctor's office and is immediately transmitted to the health insurer, in a completely paperless process. Over 50 million French citizens currently use their Sesame Vitale smart cards.

The network that supports the Vitale system is accessed through a national secured extranet operated by a private telecommunications company. Two smart cards are required for access, one for the patient (the Vitale card) and one for the provider (the Health Professional Card). The electronic transaction can also be transmitted via a different network, using Internet standards. For security reasons, however, data sent to the mandatory insurer must be input through the secured network. The information contained in each health professional's card varies by provider specialty, allowing providers to access only relevant portions of the patient's file. The system also allows for electronic signatures and eligibility verification.

The results of the program have been striking:

- Over 1 billion euros per year in savings
- Better control over expenditures
- Increased privacy
- Faster settlement of healthcare claims, often in just a few days

In addition, the government has been able to build up statistics on pathologies.

One of the major goals of smart identification cards was to empower citizens and also to provide a non-contestable identity document to limit fraud. By eliminating the need for an individual to verify identity—a major cost component of traditional systems—the cost of delivering services has been reduced dramatically. The use of smart cards has also increased national security and created a "feedback" loop with citizens.

6.7 German Health Card

In January 2006, each of the 71 million legal customers of health insurance in Germany will receive a health smart card. This smart card is a tangible symbol of the government's ambitious plan to create ubiquitous data exchange in the healthcare industry. The project to develop and introduce the electronische Gesundheitskarte (eGK) or electronic health card is being described as one of the largest IT projects in the world, costing an estimated 1.6 billion euros.

The eGK project builds on four earlier pilots in Germany. The project uses the Internet as the backbone and incorporates a shared common platform. The platform provides communication and information sharing between various entities, extending the protocols and interfaces defined by the bIT4health pilot project that preceded the eGK project. The fundamental information component is an electronic health record (EHR); smart cards enable authentication, authorization, and secure data storage. Two cards are involved. One card will hold patient-specific applications and the cardholder's prescriptions (eRezept). The second card will be issued to healthcare professionals and medical service providers. This card will serve as a general service certificate for all persons in the medical community (medical doctors, curators, nurses, and pharmacies). It will also support cryptographic capabilities for digitally signing medical documents and prescriptions.

Because the Internet is the network backbone, patient information can be retrieved anywhere in the world. Several methods are available for interacting with the EHR. Medical data can be stored on the patient's medical card or on the servers on which the application services reside. Access to the application services takes place over a secure communications infrastructure made up of multiple virtual private networks, each catering to a different sector of the healthcare system, such as doctors or pharmacists. The communications infrastructure is protected by access and service gateways. This helps ensure that only authorized persons can gain access to the infrastructure, to the application services, and ultimately, to the data.

Medical staff and patients can communicate with the system via a Web browser or client application, providing secure and flexible access to critical emergency data. Authorized mobile clients, such as portable electrocardiographs, electronic diabetes diary applications on a PDA, or medical equipment, can store information directly to a patient's record. Appliances for home monitoring are in development, along with other smart mobile medical devices that can be operated by the patient. Information is exchanged with health insurance systems using standardized application programming interfaces, ensuring that the EHR information is dynamic and useable by all entities in the working environment.

Smart cards provide a convenient and secure medium for storing medical information. The German healthcare implementation is evaluating using the card in the following six broad categories based on the type and amount of information being stored:

- Insurance cards – containing patient ID and policy information
- Emergency medical cards – containing medical and contact information tailored to the needs of emergency medical personnel
- Hospital admission cards – containing comprehensive insurance and demographic information
- Follow-up cards – storing medical data tailored for specialties such as cardiology, diabetes, dialysis, maternity, pharmacy and oncology
- Universal health cards – containing insurance ID information, key demographic data and link to the patient's medical record

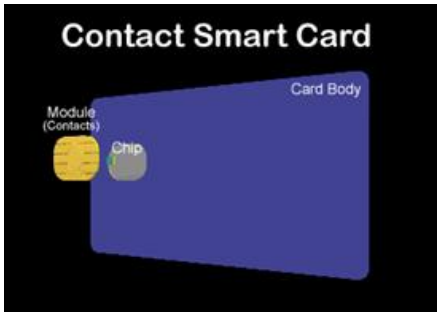
The eGK is targeted for rollout in 2006, as legislated by the German government. The Germans have decided to include prescription information on the card as the first application. No final decision has been made on whether the card, which will include all of the security features of today's smart card technology, will also carry a digital signature.

7 Appendix II: Smart Card Technology Overview

A smart card is a device that includes an embedded integrated circuit chip (ICC). The chip can be either a microcontroller with internal memory or a memory-only chip. The card communicates with a reader, either through a physical connection (a contact smart card) or a remote contactless interface (a contactless smart card). Smart cards are available in a variety of form factors, including plastic cards, fobs, subscriber identification modules (SIMs), and USB-based tokens.

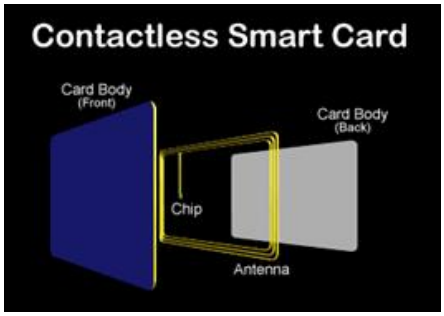
7.1 Smart Card Technology[16]

There are two general categories of smart cards: contact and contactless.



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.

A contactless card requires only close proximity to a reader. Both the reader and the card have antennae, and the two communicate over this contactless link. Most contactless cards also derive power for the internal chip from this electromagnetic signal. The range is typically one-half to three inches for non-battery-powered cards, ideal for applications such as building entry and payment that require a very fast card interface.



Two additional categories of cards are dual-interface cards and hybrid cards. A hybrid card has two chips, each with a contact or contactless interface. The two chips are not interconnected. The dual-interface card has a single chip with both contact and contactless interfaces. With dual-interface cards, it is possible to access the same chip using either a contact or contactless interface with a very high level of security.

The chips used in all of these cards fall into two categories as well: microcontroller chips and memory chips. A memory chip is like a small floppy disk with optional security. Memory chips are less expensive than microcontrollers but with a corresponding decrease in data management security. Cards that use memory chips depend on the security of the card reader for processing and are ideal for situations that require low or medium security.

A microcontroller chip can add, delete, and otherwise manipulate information in its memory. A microcontroller is like a miniature computer, with an input/output port, operating system, and hard disk. Smart cards with an embedded microcontroller have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signatures) and interact intelligently with a smart card reader.

The selection of a particular card technology is driven by a variety of issues, including:

- Application dynamics
- Prevailing market infrastructure
- Economics of the business model
- Strategy for shared application cards

Smart cards are used in many applications worldwide, including:

[16] Images provided courtesy of Gemplus.

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

7.2 Smart Card Standards

Smart cards have been implemented around the globe in a number of diverse industry segments, to satisfy a number of business needs. As these markets have matured, of necessity both low level and application level smart card standards have been developed. These standards are typically written and supported by either international organizations (such as ISO/IEC and CEN) or business organizations (such as EMVCO and APTA).

7.2.1 Low Level Standards

Two low level standards have been widely adopted, one for contact smart cards and one for contactless smart cards.

The basic contact smart card standard is the ISO/IEC 7816 series, part 1-10. ISO/IEC 7816 is a multi-part international standard that defines many aspects of a contact smart card and its interfaces, including the card's physical dimensions, the electrical interface, the communications protocols, the card file structure, and the application programming interface. The most commonly used parts are 1 through 6. These standards are derived from the financial card standards.

The primary contactless smart card standard being used for transit and financial applications is ISO/IEC 14443. ISO/IEC 14443 is an international standard that defines the interfaces to a contactless smart card, including the RF interface, the electrical interface, and the communications and anti-collision protocols. There are two parts to the standard, A and B, which describe two basic modes of operation for an ISO/IEC 14443-compliant card.

7.2.2 Application Level Standards

Many application level standards have been designed by industry groups and are used in various parts of the world. This section describes some of the more widely used standards.

7.2.2.1 Credit and Debit Card Payments—EMV 2000

The EMV specification provides a standard for credit and debit smart card applications and was developed by Visa and MasterCard. It is the standard for contact smart card payments. It is currently deployed in much of the world but is not used in the United States. The standard is managed by EMVCO.

7.2.2.2 Transit—UTFS

The UTFS specifications are currently under development. The goal is to develop a series of documents that provide industry guidance for achieving the following:

- Creation of an open architecture payment environment
- Integration of independent payment systems

These standards are managed by the American Public Transportation Association (APTA).

7.2.2.3 Government Identity Cards

As a result of Homeland Security Presidential Directive 12 (HSPD-12), issued by President George W. Bush on August 27, 2004, NIST published Federal Information Processing Standard Publication 201 (FIPS 201), *Personal Identity Verification (PIV) of Federal Employees and*

Contractors, on February 25, 2005. FIPS 201 provides the specifications for a standard Federal smart ID card, called the PIV card, that must be used for both physical and logical access and can be used for other applications as determined by individual agencies. The PIV card is a smart card with both contact and contactless interfaces. Government agencies are currently moving to implement FIPS 201-compliant systems.

7.2.2.4 Mobile Telephony – GSM SIM

The mobile phone industry has several telecommunication standards, but the predominant one globally is GSM. The GSM standard uses smart cards called Subscriber Identification Modules (SIMs) that are configured with information essential to authenticating a GSM-compliant mobile phone, thus allowing a phone to receive service whenever the phone is within coverage of a suitable network. This standard is managed by the GSM Association.

8 Appendix III: Portable Medical Records – Data Examples

There are currently several different standards for the definition of a "portable medical record." These have been discussed in Section 3.2. The most important of these is the Continuity of Care Record (CCR) defined by ASTM. The primary use case for the CCR is to provide a snapshot in time containing the pertinent clinical, demographic, and administrative data for a specific patient.

Depending on who is using the portable medical record – doctor, hospital, emergency medical staff, nurse, emergency room staff or administration – each is looking for a part of the medical record to complete their service to a patient. Because of HIPAA privacy requirements, they can no longer leave this information openly available on a desk, bed or chart holder. The standards define security measures to be taken to secure patient information so that the information on that patient will stay confidential and the patient identity is protected.

Medical information needs to be available to the acting professional seeing the patient *first* – whether the patient is being seen for life-threatening or standard medical treatment. A portable medical record is extremely important to the healthcare professional treating a patient for the first time.

8.1 The Continuity of Care Record[17]

The Continuity of Care Record (CCR) is a core data set of the most relevant administrative, demographic, and clinical information facts about a patient's healthcare, covering one or more healthcare encounters. It provides a means for one healthcare practitioner, system, or setting to aggregate all of the pertinent data about a patient and forward it to another practitioner, system, or setting to support the continuity of care.

The CCR includes a summary of the patient's health status (e.g., problems, medications, allergies) and basic information about insurance, advance directives, care documentation, and the patient's care plan. It also includes identifying information and the purpose of the CCR. The CCR may be prepared, displayed, and transmitted on paper or electronically, provided the information required by this standard specification is included.

The following is an example of the CCR record format and the data it contains. The CCR record contains the header, main body and the footer. These sections are defined as follows:

The *CCR header* consists of the following CCR sections:

- *Unique identifier* of the CCR, generated by the originating entity/system, uniquely identifies each explicit instance of a CCR.
- *Date/time* refers to the exact time the data on a specific patient were aggregated to create a CCR, which is not necessarily the time the CCR was transmitted, printed, or sent.
- *Patient* identifies the person to which the CCR refers.
- *From* identifies the practitioner(s), person(s), system(s), or organization(s) that generated the CCR and also defines the healthcare role that entity is playing when generating the CCR.
- *To* identifies the intended recipient or recipients (practitioner, person, system, or organization) of the CCR and that recipient's role in relationship to the patient.
- *Purpose* defines the specific reason that a CCR is generated, such as patient admission, transfer, consult/referral, or inpatient discharge.

The CCR body includes the following patient administrative and clinical sections.

[17] Extracted, with permission, from *ASTM E2369-05 Standard Specification for Continuity of Care Record (CCR)*, copyright ASTM International, 100 Barr Harbor Drive, West Conshohocken, PA 19428. A copy of the complete standard is available from ASTM (http://www.astm.org).

- *Insurance* contains data on the patient's payers.
- *Advance directives* contains data defining the patient's advance directives and any reference to any existing supporting documentation and the physical location of that documentation, such as a durable power of attorney for healthcare.
- *Support* lists the patient's support providers and contacts (e.g., family, next of kin, legal guardian, durable power for healthcare, clergy, caregivers, support organizations) at the time the CCR is generated.
- *Functional status* lists and describes the patient's functional status (e.g., competency, ambulatory status, ability to care for self, activities of daily living) at the time the CCR is generated.
- *Problems* contains data defining the patient's relevant current and historical clinical problems, conditions, diagnoses, symptoms, findings, and complaints at the time the CCR is generated. If the CCR is being created for a referral, they should be ranked in order of importance for the referral purpose. Otherwise, reverse chronological order of onset should prevail.
- *Family history* contains data defining the patient's blood or genetic relatives in terms of possible or relevant health risk factors.
- *Social history* contains data defining the patient's occupational, personal (e.g., lifestyle), social, and environmental history and health risk factors.
- *Alerts* contains data defining the patient's warnings such as allergies, adverse reactions, and other alerts.
- *Medications* defines a patient's current medications and pertinent medication history.
- *Medical equipment* defines a patient's implanted and external medical devices and equipment that their health status depends on, as well as any pertinent equipment or device history.
- *Immunizations* defines a patient's current immunization status and pertinent immunization history.
- *Vital signs* defines the patient's current and historically relevant vital signs (e.g., blood pressure, pulse, respiratory rate, height, weight, body mass index, head circumference, crown-to-rump length, pulse oximetry, pulmonary function tests)
- *Results* captures detailed pertinent and most recent laboratory, diagnostic, and therapeutic results data.
- *Procedures* defines all interventional, surgical, diagnostic, or therapeutic procedures or treatments pertinent to the patient historically and at the time the CCR is generated.
- *Encounters* contains data defining all pertinent healthcare encounters as well as pending healthcare appointments of the patient at the time the CCR is generated.
- *Plan of Care* contains data defining all pending orders, interventions, encounters, services, and procedures for the patient.
- *Practitioners* contains data defining all healthcare providers involved in the current or pertinent historical care of the patient. At a minimum, the patient's key healthcare providers should be listed, particularly the patient's primary physician and any active consulting physicians, therapists, and counselors.

The CCR footer contains the following sections:

- *Actors* contains data defining all of the individuals, organizations, locations and systems associated with the data in the CCR.
- *References* contains information about external references (i.e., data sources/locations that are outside the CCR).
- *Comments* contains all text comments associated with any data within the CCR.
- *Signatures* contains all signatures associated with any data within the CCR.

8.2 Portable Medical Record Example

As an example, the Florida eLife-Card program described in section 6.4 uses the following data in the portable medical record:

- Pre-existing medical conditions
- Medications/prescriptions
- Allergies/diseases/conditions
- Advanced directives (living will or Five Wishes)
- All treating physicians
- Emergency contact
- Insurance information
- Religious preference
- Radiology results
- Laboratory results
- Medical history

Many current portable medical record implementations define the information that each healthcare organization believes must be in the record. This results in improved medical care, but doesn't provide the interoperability that could result in a patient's portable medical record being truly portable. By using a standard such as the CCR, healthcare organizations can implement portable medical records that can be interoperable, portable and usable across healthcare providers and systems.