Healthcare Identity Management: The Foundation for a Secure and Trusted National Health Information Network

A Smart Card Alliance Position Paper for Government Policy Makers and Healthcare Stakeholders

Executive Summary

Policy makers are looking carefully at the best ways to improve our healthcare system with much emphasis being placed on the need for electronic health records for every American. This effort also includes creating an infrastructure to allow the exchange of these records at the regional, state and national levels. With the passing of the American Recovery and Reinvestment Act of 2009 (ARRA), the federal government is poised to invest over $19 billion in healthcare information technology (HITECH Act).[1] This investment will provide significant incentives for healthcare providers to implement electronic medical record (EMR) systems over the next five years. This action has the potential to dramatically change the landscape of modern medicine and is generally seen as a tremendous step forward; however, we must ensure that this course achieves the ultimate goals of this initiative.

If we are to improve healthcare information management, we must start with the accurate identification of each person receiving or providing healthcare services, and anyone accessing or using this information. As we move away from paper-based medical records that are controlled by physical access to buildings, rooms, and files, we need to have an infrastructure that supports strong identity and security controls. The issues with establishing identity are compounded as electronic medical records are used by many different organizations at the regional, state, and national levels. There must be a way to uniquely and securely authenticate each person across the healthcare infrastructure, whether that interaction is in person or over the Internet.

Until now, there has been a slow and uncoordinated transition toward electronic medical records. There are a myriad of systems on the market today, each with its own methods for handling patient and record identification and each with varying levels of security and privacy controls. Many systems rely on simple usernames and passwords to identify and control access. Far fewer implement strong multi-factor authentication (such as smart cards). It is critical that a set of standards be established for identifying the patient, the medical provider, and all others handling electronic records so that information across different locations can be shared easily and securely and so that patient privacy is maintained. Accurate identification and authentication seem like capabilities that should already exist in healthcare; however, identification and authentication are currently uncontrolled and not standardized among medical systems, locations, and organizations within the healthcare community.

This paper introduces the current challenges and explains why identity management in healthcare is an essential and foundational element that must be made a priority by policy makers in order to achieve the goals of widespread use of electronic health records to support the secure and seamless exchange of healthcare information. The paper also recommends best practices for introducing a healthcare identity management infrastructure – one that provides the needed security and privacy controls that should be specified by policy makers. The healthcare industry has the opportunity to leverage and build upon existing federal initiatives and standards, such as NIST SP 800-63, *Electronic Authentication Guideline*, Federal Information Processing Standard (FIPS) 201 and the Personal Identity Verification (PIV) card, which are already in use by numerous government agencies.

It is crucial for government policy makers to understand the importance of identity management and the current challenges faced in healthcare today. As the national healthcare agenda moves forward, solid identity standards and technology must be employed to meet the needs of patients and providers and ultimately to support the creation of a national health information network for the United States. The Smart Card Alliance recommends that smart cards be used as a foundational technology to create strong identity credentials to protect our citizens and facilitate the secure exchange of personal medical information.

The State of Healthcare Identity Management Today

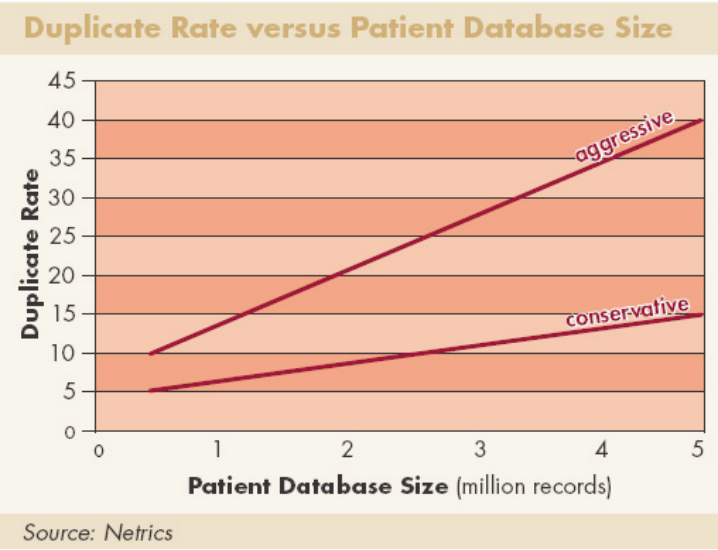
A number of converging factors highlight the need to rethink the current mode of operation in healthcare. Key areas in need of attention are: patient identity; patient healthcare record management; medical identity theft; medical fraud; patient privacy; and the security and portability of identity and healthcare records. This paper addresses each of these areas in the sections that follow and demonstrates how these issues are sapping the healthcare industry of money, performance and quality of care. In the worst case, these issues can jeopardize the safety and lives of patients. The problem at the root of these issues is the lack of consistent and uniform identity management, with a solid set of policies, procedures, and technologies. With respect to identity infrastructure, healthcare today is where the financial industry was forty years ago (think back to the days of passbook savings accounts), with mostly antiquated, paper-based systems that afforded little security or identity protections and that were expensive and labor-intensive to operate and maintain. In the current Internet-era, information on millions of citizens can be stored on a memory chip that is smaller than a postage stamp, and that data can be moved globally in seconds. Paper-based systems do not stand a chance at effectively protecting data, sharing data, or conducting commerce in today's world. To be effective, the American healthcare industry must adopt Internet-era technologies to protect its patients, providers, and payors. Smart card technology has already been globally proven to be effective at protecting identity, privacy, and commerce in today's Internet-era world, and is well-suited to the challenges of the American healthcare system.

Patient Identity and Healthcare Record Management Issues

It has been reported that over 195,000 deaths in the United States occur annually because of medical errors.[2] Of those, almost 60 percent were attributable to a failure to correctly identify the patient.[3]

Accurately identifying patients and linking them with their medical records are significant challenges today for hospitals, healthcare providers and payors, with the government representing one of the largest stakeholders in this industry. Improper patient identification can occur for many reasons including common names, misspellings, phonetic spellings, numeric transpositions, fraud, as well as patient language barriers which can lead to errors in a patient identity. These identity errors result in undesirable financial and clinical issues for the hospital, provider, and patients.

In addition to the problem of misidentification of the patient, there is also the problem of “incomplete” medical records. Studies have found that substantial numbers of duplicate medical records are created in hospitals, which means that portions of a patient’s complete medical record are spread across multiple records leading to continuity of care issues, potential delays in treatment and/or medical errors. Duplicate records can also lead to redundant or unnecessary testing, medical and billing errors, and bad claims. In smaller institutions (with patient databases of less than one million records), the duplication rate is typically between 5% – 10%, and for larger institutions (with patient database greater than four million records), duplication rates can range from 15 to 40%.[4] Correcting patient database records can be a significant expense; for large hospitals this can add up to millions of dollars per cleanup every few years. Database record cleanup is a flawed approach since it addresses the problem only after it has occurred rather than dealing with the root cause of the problem – inadequate patient identification and record matching. Unfortunately this problem grows exponentially as the number of institutions and medical providers for a single patient increases.[5]



Beyond the Hospital Walls: The Challenge of Moving to Regional and National Records and Networks (EMR-EHR-RHIO-HIE-HIO-NHIN)

Looking at the strategies to handle patient record matching being employed by Regional Health Information Organizations (RHIOs) and Health Information Exchanges (HIEs) across the country, a core component of their architectures hinge on the use of a record locator service (RLS) which essentially creates a master patient index across all of the partnering institutions' patient databases. Typically this use involves the imprecise method of statistical matching, in which a number of demographic elements (e.g., name, date of birth, zip code, Social Security number) are compared, and based on a probabilistic model, it is determined whether the records match based on a prescribed confidence level. If this confidence level is set too low, false positive matches (matching records that are not for the same patient) are likely. If the confidence level is set too high, many false negatives (records that are for the same patient but not linked due to lack of sufficient demographic data) will result. Both scenarios present challenges to the healthcare industry. False positives can create very serious issues when two distinct patient records have been merged or overlaid. The consequences can be dire since a physician could be looking at the wrong medical history or test results, and then prescribing medication or treatments for the wrong patient. False negatives have the effect of fragmenting the patient's medical record and excluding potentially valuable information from the patient's chart. Unfortunately, statistical methods can never achieve 100% accuracy and always carry a margin of error. It is for this reason that many groups have called for the adoption of a (potentially national) unique patient identifier (UPI).[6,7]

A recent RAND report (2008) entitled "Identity Crisis" highlights many of the issues associated with statistical matching, makes the case that identity management is a major challenge for the U.S. healthcare system, and calls for a unique patient identifier.[8] Some privacy groups have been opposed to a unique patient identifier, suggesting that use of a UPI would make it easier to access protected health information and provide less security for a national healthcare network. However, the real privacy issue is not the use of a UPI, it is the lack of an identity management infrastructure and associated security mechanisms to protect systems that store or have access to protected healthcare information.

Medical Identity Theft and Fraud

Medical identity theft and fraud are significant and growing problems in healthcare. The U.S. National Health Care Anti-Fraud Association (NHCAA) estimates conservatively that 3% of all healthcare spending—or $68 billion—is lost to healthcare fraud each year.[9] Other estimates by U.S. government and law enforcement agencies place the loss as high as ten percent of our annual expenditure, or $200 billion, and growing.[10] The U.S. Department of Health and Human Services defines medical identity theft as "the misuse of another individual's personally identifiable information such as name, date of birth, Social Security number, or insurance policy number to obtain or bill for medical services or medical goods." A recent Harris Interactive Poll estimated that nine million adult Americans, or four percent of the population, believe that they or a family member have lost confidential personal medical information or had the information stolen.[11]

As our nation moves from a predominantly paper-based record system to electronic health records, implementing strong security measures, including strong authentication of those individuals requesting access to medical records, is crucial for patient privacy. Current HIPAA requirements try to address this problem; however, they miss the critical point of requiring strong identity assurance of all parties that have access to healthcare information (patient, provider, payor).

Unlike other forms of identity theft, once medical information is compromised and in the wrong hands, the loss of the data is irreversible and the consequences can affect the victim for a lifetime. The security required for personal health information is far different from other types of personal information. For example, if credit card information is stolen and results in unauthorized purchases, the affected consumer is protected from liability. Today, if an individual's health information is exposed, it can have a lasting negative impact and affect future employment and insurability – with no policies and procedures in place to address the theft. Medical records are highly sensitive collections of personal information and warrant the highest confidence in their accuracy and integrity and the highest security and privacy protections.

Efforts to Improve Healthcare Information Management

Improving healthcare information management often focuses on exchanging patients' electronic medical records over the Internet at the regional and state level via HIEs and RHIOs, and then connecting the nation's HIEs and RHIOs to form the National Health Information Network (NHIN). However, focusing on information exchange puts the cart before the horse. The benefits of wider information exchange will not be realized without a solid identity management foundation. Worse, accurately linking patient records gets exponentially harder as the size of the patient population grows, and resolving identity questions is very difficult without a solid identity infrastructure that supports strong authentication of an individual's identity. What this means in real terms is that, were a NHIN to be established without forethought given to personal identity management, it would become virtually impossible to correct the infrastructure after the fact. Identity is an issue that must be addressed early in the process for projects like NHIN to succeed.

A solid identity management foundation also produces many other benefits to patients, healthcare providers, payors, regulators and other stakeholders. These include reducing the risk of medical errors, lowering healthcare costs, and stemming fraud and healthcare identity theft. For these reasons, a solid identity management infrastructure needs to be a foundational element of the solution.

A Solution for the Healthcare Identity Crisis

It is evident that one of the key tasks in creating healthcare policy is to solve the problems of properly identifying patients and healthcare providers, matching healthcare records, and identifying those that have authorized access to them. An identity management solution is not the silver bullet for all patient and electronic medical record management problems; however, it is the cornerstone for any solid solution to be implemented.

We firmly believe that smart cards provide the easiest, most cost-efficient, secure, and user-accepted method for solving the healthcare identity management problem

A smart card looks very much like a typical credit card, but what makes it "smart" is the small computer chip built into the card. Unlike magnetic stripe or RFID cards, the smart card's computer provides high levels of security and privacy protection, making the technology ideal for complying with the HIPAA/HITECH mandates and preventing fraud or false identification. Smart cards can be readily used online and across networks and deliver very high levels of security over the Internet. They are also very convenient and easy for people to use.

Smart card technology is well established in the United States as a standards-based, secure and privacy-sensitive technology platform for identity applications. Smart card technology is currently used in the Department of Defense Common Access Card (CAC), the Federal Information Processing Standard (FIPS) 201 Personal Identity Verification (PIV) card being issued to all federal employees and subcontractors, the Transportation Worker Identification Credential (TWIC), and the U.S. electronic passport. Existing standards (e.g., FIPS 201) are enabling corporations and state and local governments to issue smart card-based identity credentials that are interoperable with those used by the Federal government. Many countries around the world already have smart card-based healthcare ID cards, including France and Germany who have issued over 140 million smart health ID cards to their citizens.[12]

The following examples illustrate how smart health cards address several key healthcare challenges.

> **Smart Cards and the Unique Patient Identifier (UPI).** Many organizations agree that there is a strong need for a UPI to link medical records across multiple institutions and within multiple departments in large institutions. The smart card can be used to securely hold the UPI, along with other identity information, and to provide two-factor or three-factor authentication. Smart card technology enables distributed and federated applications in lieu of a central database of all patient identities and personal information. The use of smart cards and federated data with standards-based protocols would allow medical practitioners to have access to data across multiple data stores with an assurance that: a) the patient identity is verified; b) the records retrieved match the patient; and c) only those that have need of the data have access to it. In the case of data access, proper security controls must also be implemented around the

applications, databases, and environments that house electronic medical data. Smart cards can be effective in supporting healthcare applications with or without a unique patient identifier. Smart cards can serve as a secure way to aggregate multiple identifiers across many different systems or organizations, linking them all on the smart card.

Smart Cards and Form Factor. It is critical that the healthcare identity solution support many different medical environments and is in a form factor that is easily adopted by U.S. citizens. Currently, most insurance companies issue some form of card to their clients to identify them as policy holders and to provide some level of information required by medical staff for billing. Most medium to large medical institution uses ID cards as part of their core infrastructure for identifying medical staff. In addition, the Department of Homeland Security uses FIPS 201-interoperable smart cards to identify emergency responders, who are often the same medical staff employed and credentialed by medical institutions. The smart card provides a secure card-based form factor that can be widely accepted throughout the infrastructure.

Smart Cards and Emergency Medical Information. Smart cards also provide a secure way to store portable patient data, such as a medical history including current medications, allergies, and blood type that could be critical information in case of an emergency. Emergency medical staff could access this vital information immediately from a patient smart card at the scene and have that information transferred to the hospital while en route. The ability of the patient to carry a portable medical summary with them at all time is extremely valuable. In a disaster scenario, access to the information on the patient smart card could save lives during such emergency situations where time is critical and availability of computer networks may be compromised.

Smart Cards: Medical Identity Theft and Medical Fraud. Smart card technology supports capabilities that can help address medical identity theft and fraud. Patient identification information can be securely stored on the smart card chip which has built-in tamper-resistance features that make it extremely difficult to duplicate, hack or forge. Smart cards support advanced cryptographic methods to secure data on the card. Smart cards can be used as secure tokens to provide authenticated access to healthcare information. Smart cards can also be used in conjunction with biometrics to provide the highest levels of security. For example, a healthcare provider could have a biometric template stored and matched on their smart card to provide three factors of authentication, preventing an unauthorized person from accessing, stealing or misusing patient identification.

Implementing a Healthcare Identity Management Infrastructure

An identity and authentication solution based on smart card technology provides a foundation for improving healthcare information systems in a secure, privacy-sensitive way. This foundation can be put in place without reinventing the wheel. The Federal government has already established a set of best practices, standards and technology solutions for smart card-based identity management and authentication that can be adapted to healthcare. The use of a healthcare-focused version of the FIPS 201 standard as the foundation for the healthcare industry would provide a jump-start to the definition of a national healthcare identity management infrastructure and provide a proven model for interoperability across multiple organizations.

Whatever its design and scale, healthcare IT systems will have multiple databases that store an individual's entire medical record, contact information and benefit eligibility. What is needed is a set of healthcare identity credentials that allow secure, authenticated and authorized access to that record, and that ties each person to the correct record while protecting their privacy.

A secure healthcare identity credential based on smart card technology is an ideal way to achieve HIPAA compliance and meet the more stringent requirements of ARRA/HITECH. Smart card technology provides a significantly more secure way for people to access their own healthcare information over the

Internet and for healthcare providers to access patient records. In addition, people can better control who has access to their personal and healthcare information. A smart card-based identity management infrastructure could also provide a standards-based approach for establishing trusted identity among organizations.

Smart card technology can help make the critical capabilities needed in the healthcare infrastructure both possible and cost-effective:

- Hospitals and medical providers can use a single technology platform for securely identifying employees, contractors, service providers, and patients to electronic records systems.
- Patients can use this technology to ensure security and privacy for their personal and medical information, regardless of whether it is hosted locally, at their doctor's office, or even in the "cloud" with a third-party provider such as Google or Microsoft.
- Medical insurance providers can use this technology to strongly control and audit access to patients' medical and financial information, and to identify and track service providers' activities and billing, reducing errors and preventing fraud and abuse.
- By using a single set of technology and technology standards, all three groups – medical providers, patients, and payors – can realize reduced costs and greater functionality than by employing "stove piped" solutions to individual problems.

Conclusion: The Most Important Considerations for Policy Makers

The most important point to recognize is that identity management is a fundamental issue for the healthcare industry, and that any efforts to improve healthcare information systems, reduce administrative costs, fight healthcare fraud and identity theft, and improve patient care must start by building a solid healthcare identity foundation. Existing federal government standards and industry-proven technologies can be used to create a solid healthcare identity management infrastructure and implement flexible, secure and cost-effective healthcare ID credentials.

The Smart Card Alliance recommends that smart cards be used as a foundational technology to create strong identity credentials to protect our citizens' identities and facilitate the secure exchange of personal medical information.

- Electronic medical records are necessary but not sufficient to create a national framework**.**
- Healthcare identity management is a foundational need for the success of many efforts in healthcare, such as provider EHR implementations, personal health records and health record banks, and the NHIN.
- Progress has been made by government programs to establish secure identity management standards and procedures. These efforts should be leveraged for healthcare.
- Smart card technology can provide a highly secure and privacy-sensitive platform to support an identity management framework for healthcare.

Additional information is available online at www.smartcardalliance.org.

Smart Card Alliance White Papers

Healthcare CFO's Guide to Smart Card Technology and Applications

HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements

Smart Card Technology in Healthcare: Frequently Asked Questions

Smart Cards in U.S. Healthcare: Benefits for Patients, Providers and Payors

Privacy, Identity, and the Use of RFID and RF-Enabled Smart Card Technology

About the Smart Card Alliance Healthcare and Identity Councils

The Smart Card Alliance Healthcare Council brings together payors, 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 the how smart cards can be used and to work on issues inhibiting the industry.

The Identity Council is focused on promoting the need for technologies and usage solutions regarding human identity information to address the challenges of securing identity information and reducing identity fraud and to help organizations realize the benefits that secure identity information delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology.

Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

Glossary

EHR (Electronic Health Record)
An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one healthcare organization. This is highly dependent on having interoperability between the EMR systems that house the primary data.

EMR (Electronic Medical Record)
An electronic record of health-related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff within one healthcare organization.

FIPS 201 (Federal Information Processing Standards Publication 201)
A United States federal government standard that specifies personal identity verification (PIV) requirements for Federal employees and contractors. In response to Homeland Security Presidential Directive 12, the National Institute of Standards and Technology (NIST) Computer Security Division initiated a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems. FIPS 201 was developed to satisfy the technical requirements of HSPD-12 and was approved by the Secretary of Commerce and issued on February 25, 2005. FIPS 201, together with NIST SP 800-78 (Cryptographic Algorithms and Key Sizes for PIV), are required for U.S. Federal agencies but do not apply to U.S. national security systems. FIPS 201 defines the identity vetting, enrollment, and issuance requirements for a common identity credential and the technical specifications for a government employee and contractor ID card—the PIV card. The FIPS 201 PIV card is a dual-interface smart card that is now being issued to all Federal employees and contractors.

HIE (Health Information Exchange)
The mobilization of health information electronically across organizations within a region or community. An HIE provides the capability to securely and confidentially enable electronic transfer of clinical information among separate healthcare information systems, while maintaining the meaning of the information being exchanged.

HIO (Health Information Organization)
An organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards.

NHIN (National Health Information Network)
The infrastructure being developed to provide a secure, nationwide, interoperable health information infrastructure that will connect providers, consumers, and others involved in supporting health and healthcare.

NIST (National Institute of Standards and Technology)
The Federal agency that develops and promotes measurement, standards, and technology, http://www.nist.gov/.

PHR (Personal Health Record)
An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual.

PIV (Personal Identity Verification) cards
Smart cards being issued to all Federal employees and contractors that serve as an identity credentials and allows interoperability across government agency boundaries. The PIV card supports both physical and logical access controls.

RHIO (Regional Health Information Organization)
A health information organization that brings together healthcare stakeholders within a defined geographic area and governs health information exchange among them for the purpose of improving health and care in that community. The terms “RHIO” and “HIE” are often used interchangeably. A RHIO

is a group of organizations with a business stake in improving the quality, safety and efficiency of healthcare delivery. Many view RHIOs as the building blocks of the proposed NHIN initiative.

RLS (Record Locator Service)
An electronic index of patient identifying information that directs providers in an HIE to the location of patient health records held by participant organizations of the HIE. The technology used is analogous to EMPI/MPI (Enterprise Master Patient Index) products used by multi-facility institutions to link patient records. The techniques used are statistical matching based on probabilistic models.

UPI (Unique Patient Identifier)
A unique non-changing alphanumeric key that is associated with the identity of each patient and the medical records established for that patient. The UPI would ensure that medical records are reliably and accurately linked when exchanging medical information through any electronic network.

References

[1] On February 17, 2009, President Obama signed the $728 billion American Recovery and Reinvestment Act of 2009 (ARRA) into law. The Health Information Technology for Economic and Clinical Health Act (HITECH) provisions of ARRA in Title XIII, represents an investment of more than $19 billion towards healthcare IT related initiatives. HITECH specifically outlines how the federal stimulus money will be used to advance the design, development, and operation of a nationwide health information infrastructure that promotes the electronic use and exchange of information, but also includes significant changes in privacy and security provisions for health information technology.

[2] Healthgrades, "In-Hospital Deaths from Medical Errors at 195,000 per Year," July 2004, http://www.healthgrades.com/media/DMS/pdf/InhosptialDeathsPatientSafetyPressRelease072704.pdf

[3] Robin Hess, "Identity Crisis," For the Record, January 17, 2005

[4] Journal of AHIMA, "Keep It Clean: Optimizing EHRs Start with Ensuring Data Quality," June 2006, 77/6

[5] AHIMA. "Managing the Integrity of Patient Identity in Health Information Exchange," Journal of AHIMA 80, no.7 (July 2009): 62-69

[6] Barry Hieb, M.D., “The Case for a Voluntary National Healthcare Identifier,” Journal of ASTM International, February 2006, Vol. 3, No. 2

[7] NAHIT, "Safety in Numbers: Resolving Shortcomings in the Matching of Patients with their Electronic Records," December 2007, http://www.nahit.org/images/pdfs/PatientIdentifierPointofView.pdf

[8] Rand, Identity Crisis: An Examination of the Costs and Benefits of a Unique Patient Identifier for the U.S. Healthcare System 2008, http://www.rand.org/pubs/monographs/MG753

[9] NHCAA, "The Problem of Healthcare Fraud," http://www.nhcaa.org/eweb/DynamicPage.aspx?webcode=anti_fraud_resource_centr&wpscode=TheProblemOfHCFraud

[10] Federal Bureau of Investigation, "Financial Crimes Report to the Public, Fiscal Year 2007," http://www.fbi.gov/publications/financial/fcs_report2007/financial_crime_2007.htm

[11] Harris Interactive, "Millions Believe Personal Medical Information Has Been Lost or Stolen," July 15, 2008, http://www.harrisinteractive.com/harris_poll/index.asp?PID=930

[12] Smart Card Alliance, "Smart Card Technology in Healthcare: Frequently Asked Questions," May 2009

[13] NIST, NISTIR 7611, "Use of ISO/IEC 24727: Service Access Layer Interface for Identity (SALII): support for development and use of interoperable identity credentials," August 2009, http://csrc.nist.gov/publications/nistir/ir7611/nistir7611_use-of-isoiec24727.pdf