Getting to Meaningful Use and Beyond: How Smart Card Technology Can Support Meaningful Use of Electronic Health Records

A Smart Card Alliance Healthcare Council Publication

Publication Date: February 2011; minor update July 2019
Publication Number: HC-11001

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

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.

TABLE OF CONTENTS

1 Abstract

Healthcare is at a pivotal point in its evolution – one that has been faced by many other industries which have made the painful transition from a paper to a digital infrastructure. The speed at which healthcare is moving toward electronic medical records has been accelerated by government legislation and incentives, but this pace may also be its downfall. Healthcare data is a sensitive and highly personal collection of information that requires extraordinary protection. At the same time, in order to derive value from electronic health records, this information needs to be readily available to healthcare providers, healthcare facilities, and even patients and their families to positively impact care quality, accuracy and cost. This seeming dichotomy of purpose makes the effective use of electronic medical records very challenging.

However, the challenge is not simply the implementation of electronic health records, but meaningful use of them, which entails a host of additional requirements for new and existing technologies in the healthcare, security and information technology industries. The U.S. government's Health Information Technology for Economic and Clinical Health (HITECH) Act (part of the American Recovery and Reinvestment Act of 2009, or ARRA) has specific meaningful use criteria requiring all healthcare entities to use certifiable technology that has the ability to transform healthcare information into a standardized, electronic, accessible, readable and usable format. The criteria also require healthcare data to be kept confidential, private and secure, accurate, shareable with patients as well as providers, mobile and exchangeable, and readily available. Smart card technology and smart card-based systems can aid in meeting these requirements.

This white paper will discuss the ways in which smart card technology and smart card-based systems can be used to support the meaningful use of electronic health records.

Overview of the White Paper

"Meaningful use" has become more than just a buzz word of the U.S. healthcare system – it has become the top priority of today's healthcare industry. In 2010, the government, healthcare organizations, consumers and technology providers came together to move toward interoperable electronic health records that can transform the healthcare industry. This white paper outlines the ways in which smart card-based systems can better position healthcare organizations and providers for meaningful use of electronic health records, while addressing many of the security and privacy challenges that come with electronic health records and health data exchange.

2 Electronic Health Records and Meaningful Use

In July 2010, the Department of Health and Human Services' (HHS) Office of the National Coordinator (ONC) issued a "Final Rule" defining and supporting "meaningful use" of electronic health and medical records (EHRs/EMRs)[1], with October 2011 set as the first cut-off date for receiving Stage 1 incentive funding. These funds are not trivial; a minimum average of $2-4 million in incentive funds will be paid to eligible hospitals, and tens of thousands of dollars to individual eligible providers, who both implement EHRs and demonstrating that they meet specific meaningful use criteria defined as a result of the HITECH Act.

While the Final Rule stimulated the healthcare industry to move forward with adoption of EHRs, it did not do much to ensure that the process of implementing new technology was done in a safe, secure and controlled fashion. Almost immediately, there were more questions than answers. For example:

- How does an institution or vendor qualify for meaningful use certification?
- How can an institution meet some of the more difficult criteria with technology that is available?
- How do institutions prevent massive security breaches like the loss of a flash drive that contained protected health data for over 280,000 Pennsylvania consumers in September?[2]

The Smart Card Alliance believes that smart card technology and smart card-based systems can help to provide answers to these questions.

2.1 Climate Change in Healthcare Technology

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 stimulated the first concerted step toward conversion of paper medical records to computerized records in the U.S. healthcare industry. However, HIPAA provided no clear roadmaps, incentives or benefits for this costly and time-consuming process over the last 15 years, so most institutions and providers made little progress. The HITECH Act of 2009, however, brought change to the industry by focusing on key areas of use of electronic medical records and mandating that healthcare institutions implement new technologies (such as smart card and other technologies). Implementation is to be done under stringent guidelines, which the government will support, both developmentally and financially.

Newsweek described this healthcare technology climate change in an online article entitled "The Smart Set," published in early 2010.[3] According to the article, "...two recent changes to health policy will likely push hospitals in the direction of smart cards. First, the stimulus package puts $19 billion toward 'utilization of an electronic health record for each person in the United States by 2014.'" The article goes on to describe how the HITECH Act integrates both incentives and penalties to put teeth in the requirements. "Moreover, new legislation, passed in 2009, steeply increases the fines for patient security breaches. Penalties that used to cap out at $25,000 can now go as high as $1.5 million. Taken together, these two changes push healthcare providers toward a system that is both electronic and secure."

The HITECH legislation will require more sophisticated security controls for handling healthcare data. Encryption, two-factor authentication, and biometrics have all been cited as examples of technologies that should be considered to secure and protect healthcare data and systems. Noteworthy is the fact that smart card technology can be used to implement all of these technologies.

---

1 "Medicare and Medicaid Programs: Electronic Health Record Incentive Program; Final Rule," Dept. of Health and Human Services, July 28, 2010, http://edocket.access.gpo.gov/2010/pdf/2010-17207.pdf

2 From https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. Breaches Affecting 500 or More Individuals: As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary: Keystone/AmeriHealth Mercy Health Plans, PA, Individuals Affected – 285,691, Date: 9/20/10, Portable Electronic Device (Flash Drive). Also reported on the Philadelphia Inquirer's website, Thursday, October 21, 2010: http://www.philly.com/inquirer/business/20101021_Medical-data_breach_said_to_be_major.html

3 "The Smart Set," *Newsweek*, February 17, 2010, http://www.newsweek.com/2010/02/16/the-smart-set.html#

Table 1. HIMSS Analytics – US EMR Adoption Model™, 2007-2010 & HITECH Goals

US EMR Adoption Model℠						HITECH Act Meaningful Use Goals
Stage	Cumulative Capabilities	2007	2008	2009	2010 Q3	
Stage 7	Complete EMR; CCD transactions to share data; Data warehousing; Data continuity with ED, ambulatory, OP	0.0%	0.3%	0.7%	1.0%	2015 Goal (Stage 3)
Stage 6	Physician documentation (structured templates), full CDSS (variance & compliance), full R-PACS	0.3%	0.5%	1.6%	2.8%	2013 Goal (Stage 2)
Stage 5	Closed loop medication administration	1.9%	2.5%	3.8%	3.7%	
Stage 4	CPOE, Clinical Decision Support (clinical protocols)	2.2%	2.5%	7.4%	10.3%	
Stage 3	Nursing/clinical documentation (flow sheets), CDSS (error checking), PACS available outside Radiology	25.1%	35.7%	50.9%	49.7%	2011 Goal (Stage 1)
Stage 2	CDR, Controlled Medical Vocabulary, CDS, may have Document Imaging; HIE capable	37.2%	31.4%	16.9%	15.4%	
Stage 1	Ancillaries - Lab, Rad, Pharmacy - All Installed	14.0%	11.5%	7.2%	6.7%	
Stage 0	All Three Ancillaries Not Installed	19.3%	15.6%	11.5%	10.5%	
Data from HIMSS Analytics™ Database © 2010		N = 5,073	N = 5,166	N = 5,235	N = 5,233	

After more than a decade of attempting to move to electronic medical records, clinical documentation and patient information, the industry had only marginal success prior to 2009 (see Table 1). The ARRA/HITECH Act, however, has kicked EMR adoption into high gear. The Final Rule for meaningful use component pushes healthcare providers and institutions to move from paper-based data and infrastructure to electronic data and networked systems – a move that corporate business, banks, law enforcement and other industries made years ago. To assist the healthcare industry with the transition, the U.S. government will also be providing incentive payments to providers and institutions that go beyond mere implementation and actually demonstrate they are meaningfully using the new technology. The government is essentially using the traditional "carrot and stick" approach to motivate healthcare industry investment in new technologies and processes. The incentives are the carrots, and the stick – a system of penalties for failing to implement and meaningfully use and exchange electronic health records and patient information – will come into play in a few years.

To qualify for incentive payments, eligible hospitals and providers must use a "qualified EHR." According to the HITECH Act, a qualified EHR must have specific technical capabilities, must support providers in achieving meaningful use objectives, and must be certified. According to HHS, the overriding reason for requiring certification for healthcare technology is to "provide assurance to purchasers and other users that an EHR system, or other relevant technology, offers the necessary technological capability, functionality, and security to help them meet the meaningful use criteria established for a given phase."[4]

One of the primary reasons smart card technology is positioned to become such an integral piece of the new healthcare technology landscape is precisely because of its ability to assist in meeting meaningful use requirements: providing the technological capability needed for providing secure storage and access to EHRs, enhancing and improving EHR functionality and workflows, and ensuring security protocols meet and/or exceed the requirements of certification.

2.2 Meaningful Use Measures and Certification

The certification criteria for health record technology final rule[5] speaks specifically to requirements all technology vendors must satisfy to meet the meaningful use criteria. There are basically two portions of the rule – the functionality requirements and the framework requirements. While the specific functionality

[4] http://healthit.hhs.gov/portal/server.pt?open=512&objID=1196&parentname=CommunityPage&parentid=6&mode=2
[5] http://edocket.access.gpo.gov/2010/pdf/2010-17210.pdf

requirements determine whether or not an EHR can be certified as "complete" or as a "module," the framework requirements are applicable to all types of healthcare technology.

The rule specifies that complete EHRs and modular EHRs must contain functionality that allows the technology to be "meaningfully used," in order to qualify for Stage 1 meaningful use certification, and thereby qualify a healthcare entity for incentive funding. The exact distinction between "complete EHR" and "modular EHR" functionality is still unclear, but the Final Rule has been interpreted by most as meaning that a complete EHR is a certified primary system for storage, manipulation, retrieval and exchange of electronic medical/health records for an organization or provider. The complete EHR provides the majority of core meaningful use components but may need to work in conjunction with additional certified ancillary technologies to satisfy all meaningful use criteria. A modular EHR is a secondary certified healthcare technology system which provides at least one core or menu of meaningful use components; the modular EHR would need to work in conjunction with a complete EHR or another modular EHR to satisfy all meaningful use criteria.

Table 2 demonstrates how smart card technology and smart card-based systems meets the needs of the 16 Stage 1 meaningful use core measures, which are mandatory requirements for EHR, EHR module and health information exchange functionality for incentive eligible hospitals (EH) and eligible providers (EP) to implement by October 2011.

The rule also includes 12 Stage 1 menu requirements, 10 pertaining to eligible hospitals, and 10 pertaining to eligible providers. Both hospitals and providers must also complete 5 out of 10 of their respective menu requirements in order to qualify for incentives, including mandatory reporting of clinical quality measures. Key menu requirements where smart card-based systems can potentially be a key factor with a modular EHR include the following:

- Use EHR technology to identify patient-specific education resources and provide those to the patient as appropriate
- Record advance directives for patients 65 years of age and older (for EH)
- Incorporate clinical lab test results into EHRs as structured data
- Send reminders to patients per patient preference for preventive or follow-up care (for EP)
- Provide patients with timely electronic access to their health information (for EP)
- Perform medication reconciliation at relevant encounters at each transition of care
- Provide summary care record for each transition of care and referral

While smart card technology on its own does not provide a complete EHR technology solution, smart card-based systems can be used by healthcare organizations to meet many of the Stage 1 core and menu requirements for meaningful use. Smart card technology is positioned to be a leading contender for designation as a modular EHR technology solution and provides many of the features and capabilities needed to comply with some of the more stringent requirements of HITECH and the later stages of meaningful use that will be phased in by 2015.[6] The integration of smart card technology with emerging EHR systems should be a top consideration for healthcare vendors looking to provide certified healthcare solutions to the marketplace.

[6] See **Federal Register** / Vol. 75, No. 144, Page 44597. "Certified EHR Technology means: (1) A Complete EHR that meets the requirements included in the definition of a Qualified EHR and has been tested and certified in accordance with the certification program established by the National Coordinator as having met all applicable certification criteria adopted by the Secretary; or (2) A combination of EHR Modules in which each constituent EHR Module of the combination has been tested and certified in accordance with the certification program established by the National Coordinator as having met all applicable certification criteria adopted by the Secretary, and the resultant combination also meets the requirements included in the definition of a Qualified EHR."

***Table 2**. How Smart Card Technology and Smart Card-Based Systems Meet Meaningful Use Criteria*

CM#	Meaningful Use Core Measure (CM)	EP/EH/ Both	Classic/ Complete EHR/EMR Solution[7]	Potential Smart Card Technology Solution	How Smart Card Technology and Smart Card-Based Systems Can Satisfy Meaningful Use Requirements[8]
1	Use a computerized physician order entry (CPOE) system	B	✓	✓	Provider smart card can be used to authenticate user onto system
2	Implement drug-drug and drug-allergy interaction checking	B	✓	▪	
3	Generate and transmit permissible prescrip-tions electronically (ePrescribing)	EP	✓	✓	Smart card can provide high assurance user authentication and can be used to digitally sign prescriptions to eliminate fraud and abuse
4	Record demographic information	B	✓	✓	Patient identity and demographics can be encrypted and stored on smart card; the data can be read and written to at point of care[10]
5	Maintain an up-to-date problem list of current and active diagnoses	B	✓	✓	Patient problem list can be encrypted, maintained and updated on smart card; can be read and written to at the point of care
6	Maintain an active medication list	B	✓	✓	Patient medication list can be encrypted, maintained, reconciled and updated on smart card; can be read and written to at the point of care
7	Maintain an active medication allergy list	B	✓	✓	Patient medication allergy list (can also include other information such as non-medication allergies, implanted devices) can be encrypted and stored on smart card; can be read and written to at the point of care
8	Record and chart vital signs	B	✓	✓	Most recent and trended patient vital signs can be encrypted, maintained and updated on smart card; can be read and written to at the point of care
9	Record smoking status	B	✓	✓	Patient smoking status can be encrypted, maintained and updated on smart card; can be read and written to at the point of care
10	Implement one clinical decision support rule and track compliance with it	B	✓	▪	

[7] The Certified HIT Product List (CHPL) provides the authoritative, comprehensive listing of complete EHRs and EHR modules that have been tested and certified under the Temporary Certification Program maintained by the Office of the National Coordinator for Health IT (ONC), http://onc-chpl.force.com/ehrcert

[8] In all examples, smart cards are mobile with the patient/provider and can have the ability to be decrypted and read by emergency first responders.

CM#	Meaningful Use Core Measure (CM)	EP/EH/ Both	Classic/ Complete EHR/EMR Solution[7]	Potential Smart Card Technology Solution	How Smart Card Technology and Smart Card-Based Systems Can Satisfy Meaningful Use Requirements[8]
11	Calculate, report and transmit CMS Quality Measures	B	✓	▪	
12	Provide patients with an electronic copy of their health information upon request	B	▪	✓	An electronic summary of health information can be encrypted, maintained and updated on smart card; can be read and written to at the point of care; patient can use smart card to access data through authorized kiosks, patient portals or printer devices
13	Provide patients with an electronic copy of their discharge instructions and procedures upon request	EP	▪	✓	Discharge instructions and procedures can be encrypted, maintained and updated on smart card; can be read and written to at the point of care at time of discharge; patient can use smart card to access data through authorized kiosks, patient portals or printer devices
14	Provide patients with an electronic copy of a clinical summary for each office visit upon request	EP	▪	✓	An electronic clinical summary of health information can be encrypted, maintained and updated on smart card; can be read and written to at the provider offices' point of care; patient can use smart card to access data through authorized kiosks, patient portals or printer devices
15	Exchange key clinical information among providers of care and patient-authorized entities electronically (e.g., health information exchanges)	B	▪	✓	Smart card technology can be used to interface with patient portals and health information exchanges and can provide, for example, a health information exchange portal between hospitals and physician offices. The smart card can also hold a detailed medical summary which can be read from the card.
16	Privacy and security: Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities	B	✓	✓	Smart card technology and smart card-based systems can implement the highest level of encryption, user authentication, privacy measures, and auditability. All exchanges of non-protected as well as protected health information (PHI) data can be encrypted during storage, transport or exchange. Network layer security and encryption can be configured end-to-end, route-to-route, or edge-to-edge. Smart cards can support PKI certificates and biometrics and follow robust security standards (ISO, NIST).

3 Fulfilling the Security Requirements of Meaningful Use

The basic security components that a Certified EHR technology must provide to meet meaningful use requirements include the following[9]:

1. Provide access control measures
2. Provide emergency access measures
3. Provide an automatic log-off feature
4. Provide an audit log
5. Ensure integrity of data
6. Provide for authentication of users and access
7. Provide general encryption standards
8. Provide encryption for all data transmitted through health information exchange channels

Smart card-based systems can help healthcare institutions and providers meet meaningful use security requirements.

Each criterion is presented in Table 3 below, along with examples of how a smart card-based system can support a healthcare provider or facility in achieving meaningful use.

Table 3: EHR Certification Criteria and How a Smart Card-Based System Meets the Requirement

	Certification Criterion	How a Smart Card-Based System Meets the Requirement
1	Assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information	Patient and provider smart cards can be used to provide strong two- or three-factor user authentication (a combination of physical smart card, secret PIN and/or biometric identification) for access to electronic health information.
2	Permit authorized users (who are authorized for emergency situations) to access electronic health information during an emergency	Authorized users (first responders[10], emergency room personnel, and other healthcare data users) can use offline portable readers to access information stored on a patient smart card. Authorized users can also use healthcare provider smart cards to authenticate themselves and confirm their right to access information.
3	Terminate an electronic session after a predetermined time of inactivity	Electronic sessions could be implemented to only be active when the provider's smart card is present.
4	Encrypt and decrypt electronic health information according to user-defined preferences (e.g., backups, removable media, at log-on/off)	A best practice for healthcare systems, whether non-protected health information (NPHI) (i.e., data that has been stripped of identifiers or that is common to a large demographic group, such as zip code) or protected health information (PHI), is for all data to be encrypted and be capable of being decrypted via standard protocols. Encryption should also be required for all ancillary devices, such as smart card readers, removable media, mobile devices, and kiosks. The smart card provides the secure mobile platform for data and can both store

[9] Federal Register 45 CFR Part 170 Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology; Final Rule Final Rule Text: § 170.302(o-w).

[10] The Department of Homeland Security (DHS), National Institute of Standards and Technology (NIST), and Federal Emergency Management Agency (FEMA) have worked together to develop specifications for the First Responder Authentication Credential (FRAC) – a secure, interoperable, smart card-based identity credential designed for the emergency management community nationwide. The FRAC is now being issued in many states to first responders. Additional information is available at http://www.smartcardalliance.org/resources/lib/ERO_Credentials.pdf.

		encrypted data and encrypt/decrypt data when it's being transmitted. Smart card-based systems can support a wide variety of encryption/decryption protocols.
5	Encrypt and decrypt electronic health information when exchanged	All exchanges of non-protected as well as PHI data can be encrypted during transport or exchange in the method described above. Network layer security and encryption can be configured end-to-end, route-to-route, or edge-to-edge.
6	Record actions (e.g., deletion) related to electronic health information (i.e., audit log), provide alerts based on user-defined events, and electronically display and print all or a specified set of recorded information upon request or at a set period of time	For portable mobile data that is stored on a smart card, smart card-based systems can provide audit logging capabilities.
7	Verify that electronic health information has not been altered in transit and detect the alteration and deletion of electronic health information and audit logs	Smart card-based systems can support digital signatures and other cryptographic techniques that can enforce non-repudiation and provide high data integrity.
8	Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information	Patient and provider smart cards can be used to provide strong two- or three-factor user authentication to electronic health information (using a combination of physical smart card, secret PIN and/or biometric identification), and be used by the smart card-based system to determine authorization to access information.
9	Verify that a person or entity seeking access to electronic health information across a network is the one claimed and is authorized to access such information	Patient and provider smart cards can be used to provide strong two- or three-factor user authentication to electronic health information (using a combination of physical smart card, secret PIN and/or biometric identification), and be used by the smart card-based system to determine authorization to access information.
10	Record disclosures made for treatment, payment, and healthcare operations (optional)	Discharge information can be stored securely on the smart card or the smart card can be used to securely access discharge information on a healthcare portal.

3.1 Smart Card Solutions and Data Security, Identity Management and Data Exchange

Smart card technology can help meet many meaningful use requirements. However, smart card technology also provides unique capabilities that address specific functional gaps in the offerings of existing EHR products on the market.

Current systems have functional gaps addressing data security, identity management, and data exchange across networks. This section describes how smart card technology can be used to support healthcare providers and organizations to address these areas and satisfy the HITECH Act's meaningful use requirements.

3.1.1 Data Theft

It is no secret that data theft is the fastest growing Internet crime. And within the identify theft realm, healthcare data theft is rising faster than any other sector, a 112% increase from 2008 to 2009.[11] According to a recent Ponemon Institute study, nearly 1.5 million Americans have been victims of medical identity theft with an estimated total cost of $28.6 billion – or approximately $20,000 per victim.[12] In

[11] "EMR Data Theft Booming," *InformationWeek*, March 26, 2010, http://www.informationweek.com/news/healthcare/security-privacy/showArticle.jhtml?articleID=224200494

[12] Survey conducted by the Ponemon Institute, February 2010.

addition, the latest Ponemon Institute study finds that "data breaches of patient information cost healthcare organizations nearly $6 billion annually, and that many breaches go undetected."[13]

With the country's push toward electronic medical records, healthcare is quickly becoming a major target of cybercrime and the industry is seeing a tremendous increase in data breaches.

The specific area of data security and/or the relevant criteria from the HITECH Act are described as "Meaningful Use Stage 1 Objectives," including "protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities."

The way to stop medical identity theft is to improve patient and healthcare provider identity verification and provide enhanced data protection. Strong identity proofing at the time of enrollment, along with ongoing user authentication and data encryption are methods that can achieve these goals. To address medical identity theft, solutions need to provide higher levels of assurance than today's processes, whether the interactions are in person or remote. Solutions that incorporate smart card technology can be used to address the security and privacy challenges facing the healthcare industry.

Strong user authentication is a critical step in addressing medical identity theft. All personal health record (PHR) providers, health record banks, health insurance and hospital Web portals should provide two-factor authentication mechanisms to their end users to help secure access to personal health information. In two-factor authentication schemes, individuals typically use a card, token or mobile device to access their health information or prove identity when obtaining healthcare services. The safest and most secure two-factor methods are based on smart card technology, where a tamper-resistant chip with security software is embedded into the card, token or mobile device (like a mobile phone). A smart card allows patients to unambiguously identify themselves to their healthcare provider when accessing patient records or requesting healthcare services.

Data encryption also plays an important role in the protection of protected health information (PHI) and is now mandated as part of the breach notification laws. Encrypting PHI protects against access by intruders; smart cards provide a robust set of encryption-enabling capabilities including key generation, secure key storage, hashing and digital signing.

Smart cards also add strong authentication capabilities that ensure only authorized users are able to access PHI. These capabilities can be used by a healthcare system to protect privacy in a number of ways. A doctor can use a smart card to digitally sign orders or prescriptions, protecting the information from subsequently being tampered with and providing assurance that the doctor was the originator of the information. The fact that the signing key originated from a smart card adds credibility and a greater legal stature to the record. The smart card provides two major benefits: one, it securely holds and protects the keys; and two, it is portable, so it stays with the doctor and not in the computer where someone else might be able to fraudulently use it.

Smart cards can also put patients in control of their private information. Patients can use their smart card to securely store personal health information, authorize provider access to that information, and secure transmission of data to healthcare systems.

Issuing secure patient and provider identity credentials based on smart card technology will help to reduce medical identity theft, and will also bring numerous efficiencies to existing healthcare administration systems. Authentication solutions based on smart card technology will provide an ideal foundation for improving the security and privacy of health information systems and electronic health records.

[13] "New Ponemon Institute Study Finds Data Breaches Cost Hospitals $6 Billion; Patient Privacy in Jeopardy," *FierceHealthcare*, November 9, 2010, http://www.fiercehealthcare.com/press-releases/new-ponemon-institute-study-finds-data-breaches-cost-hospitals-6-billion-pa

3.1.2 Identity Management

In December 2008, the HHS ONC issued a Nationwide Privacy and Security Framework that established a set of principles to govern health information exchange (HIE).[14] The ONC established two Health IT Policy Committee workgroups to specifically address privacy and security in EHRs: the National Health Information Network (NHIN) and the Privacy and Security Tiger Team. In a NHIN workgroup presentation in early 2010, they suggested five essential elements that would overarch this trust framework in enabling a national health information exchange: (1) agreed-upon business policy and legal requirements, (2) transparent oversight, (3) accountability and enforcement, (4) identity and authentication, and (5) minimum technical requirements.[15]

While each of these elements is important to create this trust, none of them individually is sufficient to create the total required framework. A strong combination of all listed elements is intended to provide a foundation for this framework, creating security and confidence for providers, payers, and patients and the freedom to move information within public and private exchanges.

Identity management is the foundation of the entire future of healthcare data management. With respect to the identity management 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.

Two important issues to address in healthcare identity management are: initially establishing the correct patient identity; and then providing ongoing patient and provider authentication when accessing electronic health records.

3.1.2.1 Patient Identity

It has been reported that over 195,000 deaths in the United States occur annually because of medical errors.[16] Of those, almost 60 percent were attributable to a failure to correctly identify the patient.[17]

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 December 2010, the ONC Privacy and Security Tiger Team held a hearing on patient matching, also known as patient identity management. Part of the work of the Privacy and Security Tiger Team is to provide policy recommendations on privacy and security issues associated with linking or matching patients to their information within healthcare entities in order to support information exchange across healthcare entities.

---

[14] http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf

[15] Comments made by David Lansky, Chair, HIT Policy Committee, ONC, Department of Health & Human Services, April 21, 2010 presentation on “HIE Trust Framework”

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

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

According to the published presentation[18], information exchange between different healthcare entities depends on an ability to match patient identities without benefit of common identifiers. The presentation highlights the following:

- Correctly linking patients to their health data is a vital step in quality healthcare;
- Accuracy, integrity and quality of the patient data are also critically important; and
- Internal data issues must be resolved before tackling the larger issues involved in exchange.

The presentation concludes by stating the role of the ONC in privacy and security in patient identity is to:

- Broaden the discussion to cover data quality
- Define and understand the ecosystem and patient linkage opportunities
- Shift emphasis to data quality
- Support conversation about development of standards for minimum data set
- Promote transparency and consumer education/communication (addressing) a process for sharing how patient matching is conducted, accuracy of the matching, and challenges in health information exchange

3.1.2.2 Identity Authentication

Multi-factor authentication is critical in verifying patients and providers when accessing electronic health records. The United States Office of Management and Budget (OMB) has defined four specific levels of identity authentication "assurance" for establishing: "1) the degree of confidence in the vetting process used to establish the identity of the individual to whom a credential is issued (covered in Section 3.1.2.1 above) and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued."[19] The National Institute of Standards and Technology (NIST) developed electronic authentication guidelines for implementing the OMB-defined levels of assurance.[20] While these guidelines are currently in use within U.S. government agencies,[21] they are best practice models for use in defining authentication policies and practices for other programs. According to the October 15, 2010, ONC Privacy and Security Tiger Team meeting presentation,[22] the Tiger Team is considering tailoring this NIST/OMB e-authentication framework for use in healthcare information exchange. Within the currently-defined OMB and NIST guidelines:

- Password tokens can satisfy the assurance requirements for Levels 1 and 2.
- Soft cryptographic tokens may be used at authentication assurance Levels 1 through 3, but must be combined with a password or biometric to achieve Level 3.

---

[18] http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_7258_2833_19477_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/slides_pstt_121010.ppt

[19] `OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," December 16, 2003, available at: http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[20] "Electronic Authentication Guideline," NIST Special Publication 800-63, April 2006, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

[21] "CMS System Security and e-Authentication Levels by Information Type," CMS, April 20, 2010. CMS has defined eleven information types processed on or by CMS information systems. For each information type, CMS used FIPS 199 to determine its associated security category by evaluating the potential impact value (i.e., high, moderate, or low) for each of the three FISMA/FIPS 199 security objectives (i.e., confidentiality, integrity and availability). For each information type, CMS also used OMB M-04-04 to determine its e-Authentication assurance level (i.e., Levels 1−4) by evaluating the degree of authentication confidence required to protect the information. The results of these determinations, which apply to all CMS information and information systems, are included in the document at https://www.cms.gov/informhasationsecurity/downloads/ssl.pdf .

[22] ONC Privacy and Security Tiger Team Meeting, Discussion Materials, October, 15, 2010, http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_7258_2833_19477_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/authentication_for_hie_v9_draft.ppt

- One-time password devices are considered to satisfy the assurance requirements for Levels 1 through 3, and must be used with a password or biometric to achieve Level 3.
- Hard tokens (such as smart cards) that are activated by a password or biometric can satisfy assurance requirements for Levels 1 through 4.

Deven McGraw, co-chair of the Privacy and Security Tiger workgroup, said at the group's November 12, 2010, meeting, "We have a lever in certification to make sure the systems have the capability to be authenticated and digitally credentialed." Later in the meeting, workgroup member Dixie Baker affirmed that: "eventually we're going to have to put in place a standard and security and certification criteria for two factor authentication of EHRs."[23]

Electronic prescribing regulations already mandate a minimum of Level 3 authentication standards.[24] One could extrapolate from this that access to sensitive PHI data (for example, related to conditions or treatments such as psychiatric, cancer or HIV, or health records of celebrity or publicly recognizable patients) could warrant Level 4.

As an increasing amount of information is stored online and wider access to it is achieved, strong authentication and auditability of access rights to confidential medical information will be critical for the healthcare identity management infrastructure.

3.1.2.3 Smart Cards and Identity Management

A smart card can be used to securely hold patient 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 identity and other 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 authenticated; 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.

3.1.3 Data Exchange

The idea of data exchange is at the very core of the federally funded NHIN. The NHIN is essentially a network of networks established to allow unrestricted flow of medical information by and among certified (authenticated) healthcare providers. Elemental to safe data exchange is data privacy. According to the Health Information and Management System Society (HIMSS) web site:

> *"Information and data exchange is a critical to the delivery of quality patient care services and effectiveness of healthcare organizations. The benefits of appropriate sharing of health information among patients, physicians, and other authorized participants in the healthcare delivery value chain, are nearly universally understood and desired. A RHIO, or regional health information organization, is a group of organizations with a business stake in improving the quality, safety and efficiency of healthcare delivery that comes together to exchange information for these purposes. The terms RHIO and Health Information Exchange, or "HIE, are often used interchangeably."*

In April 2010, the NHIN Direct workgroup was established, with the directive to "create the set of standards and services that with a policy framework enable simple, directed, routed, scalable

[23] HHS Privacy and Security Tiger Team Meeting Transcript, November 12, 2010, available at: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_7258_2833_19477_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/2010_11_12_tiger_transcript_draft.pdf

[24] Code of Federal Regulations, **21** § 1311.105

transport over the Internet to be used for secure and meaningful exchange between known participants in support of meaningful use."[25]

In a White House report published on December 8, 2010 by the President's Council of Advisors on Science and Technology (PCAST), ONC and CMS were directed to develop the technical definitions and descriptions for the standard language and include them in requirements for meaningful use of electronic health records in 2013 and 2015.[26] The administration is absolutely committed to achieving interoperability, and it's "not a minor issue" for them, Blumenthal said at a standards committee meeting on December 17, 2010. "We are going to move forward with a great deal of aggressiveness on health information exchange and interoperability, and even faster than we had expected based on the council's report," Blumenthal said.[27]

However, he added, it will be up to the committee to pick a path that is "technically as refined and as open to innovation, but as reliable, as we can make it." John Halamka, co-chair of the Health IT Standards Committee noted that all data exchanges "would have to incorporate patient privacy protections."[28]

Thus, data exchange is predicated on the ability to secure data and to provide authenticated access to the data by authorized parties. Information must not only be protected during transit, but also while "at rest" on systems. Encryption and multi-factor authentication are critical to the data exchange processes, which, as described in Section 3.1.1, smart cards can support .

Data encryption and identity authentication can be managed in both small and larger ecosystems. The Federal government and other industries are using a public key infrastructure (PKI) to issue the digital certificates that are used for encryption and identity authentication, with the Federal Bridge Certification Authority enabling interoperable use across organizations. It is expected that a PKI-based infrastructure will be used in NHIN initiatives.

Another difficult challenge with health information exchange is management of the patient consent process, which allows medical information to be exchanged among providers with the permission of the patient. A smart card could be used by the patient to provide consent and give the patient control over what information is exchanged.

[25] "Direct Project HITSC Presentation," October, 2010, http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_12083_948520_0_0_18/direct-project-hitsc-oct-2.ppt

[26] http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf

[27] "Blumenthal to set aggressive pace for health data exchange," *Government Health IT*, December 20, 2010, http://govhealthit.com/newsitem.aspx?nid=75721

[28] Ibid.

4 Smart Cards: Moving from World Stage to Center Stage in the U.S. Meaningful Use of EHRs

First patented in 1974, 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 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. Smart cards have two strengths that address requirements well within healthcare: security and portability.

4.1 Smart Card Capabilities

Smart card technology used in healthcare has numerous capabilities, including the following:

- Secure storage of demographic and medical information
- Dynamic storage that can be updated in real-time
- Patient identification
- Compliance with the WEDI health identification card specification[29]
- Patient and provider authentication (PIN, biometric, signature)
- Storage of digital photograph for patient identification
- Streamlining patient throughput time, reducing paperwork and accelerating access to the medical team by providing workflow efficiencies in registration and admission
- Matching patient to a single medical record
- Integrating with legacy systems via HL7 interfaces
- Enabling search for additional medical information from external data sources
- Connectivity with physicians' offices, clinics, and networks, including access to EMRs, EHRs, and PHRs
- Integrating with kiosks for self-service check-in
- Enabling physical and logical access management
- Connectivity to patient portals including pre-registration sites
- Connectivity to third-party data storage portals such as Google Health and Microsoft HealthVault
- Ability to verify insurance information in real-time
- Ability to attach a payment source (credit/debit card, patient pay, HSA accounts)

4.2 Current Use of Smart Cards

Smart card-enabled applications are prevalent in many of today's businesses. The financial payments industry has moved to smart cards with the majority of regional financial organizations worldwide mandating that financial credit and debit cards be smart cards by a specific date. In addition, contactless smart card technology has been rapidly accepted for fast, convenient, and secure credit and debit payment transactions. Enterprises are issuing smart ID badges to employees to secure physical and logical access, and many government identity programs around the world are issuing smart card-based identity credentials to citizens.

[29] http://www.wedi.org

Countries throughout Europe and Asia are providing their citizens with smart health cards. Table 4 lists examples of national smart health card deployments worldwide; in addition to the countries listed, smart health card programs are also active in other countries, including China, Finland, Jordan, Poland, and Turkey.

Table 4: Global Smart Health Card Implementations[30]

Country	Card Type	Number of Cards	Launch Year
Algeria	CNAS	7 million	2007
Austria	e-card	11 million patient 24,000 professional	2005
Australia	Medicare Smartcard	40,000 patient	2006
Belgium	Social system identity	11 million	1998
France	Sesam Vitale Sesam Vitale-2	60 million (combined)	1998 2007
France	Carte DUO	Over 200,000 cards (private insurance card)	2007
Germany[31]	Health insurance card (Krankenversichertenkarte (KVK))	80 million	1996
Hungary	MOK, Hungarian Chamber of Doctors	40,000 professional	2006
Italy	Carta Nazionale dei Servizi	3 million (national services card)	2004
Mexico	Seguro Popular health insurance cards	3.7 million	2006
Slovenia	Health insurance card	2 million patient 70,000 professional	1999
Spain	Carte Santé	5.5 million	1995
Taiwan	National health insurance card	24 million patient 150,000 professional	2002
United Kingdom	NHS Connection for Health (health professional cards)	1.2 million	n/a

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.

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

[31] Germany is launching a new microcontroller-based smart health card, "Gesundheitskarte," in 2011, which will be issued to 80 million citizens and 375,000 healthcare providers.

The United States healthcare market is experiencing significant growth in smart card adoption. Many prominent healthcare organizations in the United States are implementing smart healthcare cards to support a variety of features and applications.[32] Smart cards are used by patients as authenticated identifiers to match the patient to his or her individual medical record, to store relevant patient information, and to pass admissions information into the hospital's admitting software, thereby automating the process. In addition, smart cards are being used by healthcare providers to authenticate their identities when accessing information.

Now applications including physical access, benefits verification, connection to and synchronization with disparate data sources, and payment management will lead the healthcare industry toward its goal of real-time patient identification and payments adjudication.

[32] Smart Card Alliance, "A Healthcare CFO's Guide to Smart Card Technology and Applications," February 2009.

5 Confidence Is Key to Adoption

Smart card technology is trusted worldwide to provide the highest level of identity verification, user authentication and secure data access. Although the technology is still comparatively new to the U.S. market, its proven capabilities and reputation for security and worldwide acceptance are accelerating its use in many industries including healthcare.

Smart card technology is widely used in Europe, and healthcare smart cards are in use in pilot or operational settings. "This card is my lifeline. It has all data about my medical history. So if I have a heart attack this is the card that will save me," says Hardy Sekhon, Group Director, Risk Management Canada Health Infoway, a $1.2 billion not-for-profit corporation accountable to 14 Federal/Provincial/Territorial Governments, which plans to provide interoperable EHR across Canada."[33]

Confidence in the technology is critical to meaningful use of EHRs. HHS states, "Confidence in health IT systems is an important part of advancing health IT system adoption and allowing for the realization of the benefits of improved patient care....Providers and patients must also be confident that the electronic health IT products and systems they use are secure, can maintain data confidentially, and can work with other systems to share information."[34] Confidence is key to adoption, successful integration and, ultimately, use – meaningful or otherwise – of any new technology, but especially technology used to secure healthcare information and ensure patient privacy.

5.1 EHRs and the Internet Are Not Enough

There has been great speculation about the value and return on investment electronic health records will bring to the U.S. healthcare system. Much has been predicated on the reduction of administrative and clinical costs. But these returns will not be fully realized if the security and privacy of this data cannot be assured or if these systems cannot reliably interoperate and exchange data. Although enormous progress has been made in developing standards to allow seamless exchange of data between medical record systems, a fundamental gap exists in the way patient identity is managed across these disparate systems. Accurate patient identification is critical to internal hospital operations but also to regional, state and national healthcare efforts. To achieve true health record interoperability patient records must be able to be unambiguously linked across a myriad of disparate systems to create one longitudinal patient record. A common approach is to use a record locator service to create a master patient index. Unfortunately, these statistical methods can never achieve 100% accuracy and always carry a margin of error.

A recent RAND report[35] 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 (UPI). 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.

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.[36,37] A smart card can be used to securely hold the UPI, along with other identity information, and to provide two-factor or three-factor authentication.

---

[33] From Express Pharma's article, Puzzled Over the Perfect EMR, http://www.expresspharmaonline.com/20070731/healthcare08.shtml

[34] http://healthit.hhs.gov/portal/server.pt?open=512&objID=1196&parentname=CommunityPage&parentid=6&mode=2

[35] 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

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

[37] 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

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

As electronic health records and health information exchange become more prevalent, the need to properly identity, authenticate and authorize individuals using and exchanging medical information will be paramount. Smart card technology can provide a significantly more secure way for patients to access their own healthcare information over the Internet and for healthcare providers to access patient records. In addition, patients can better control who has access to their private healthcare information. A smart card-based identity management infrastructure could provide healthcare with a standards-based approach for establishing trusted identity among healthcare organizations, their staff and their EMR/EHR systems.

6 The Financial Impact of Healthcare Technology

The benefits of using smart cards for integrating and meaningfully using EHR technology in the healthcare workflow are extensive and easily demonstrable. How do they compare to competing technologies in terms of financial implications to healthcare providers and facilities?

Average implementation costs of large, hospital-based complete EHR systems can range anywhere from high hundreds of thousands to millions of dollars; even smaller ambulatory-targeted complete EHRs can cost a small provider practice tens of thousands of dollars. Most of this cost is split between the customization required for the vendor application to accommodate and reflect the healthcare facility's particular workflows, and the hardware, software, resources and security measures needed to operate the EHR system.

While smart card-based systems are not inexpensive, they offer substantial labor and resource savings over time. Beyond that, smart cards are portable, easily readable-rewritable, and easily interface with cloud and other healthcare information exchange channels.

Some of the greatest areas of cost savings that healthcare providers and organizations can realize are associated with tangible and measurable benefits of meaningful use of smart card technology. Streamlining patient registration and admissions, reducing or eliminating data processing errors, improving workflows, curtailing fraud, possibly diminishing the number of human resources required to support processes, and providing rapid access to critical information in an emergency can all result in significant decrease in information technology expenditures for a healthcare facility. Overall, it is likely that the savings realized from these types of simplification of operations and data administration would significantly offset the upfront costs associated with integration of the smart card technology.

"The real payday for use of EMRs will come with interoperability," explains Jim Lott, Executive Vice President of the Hospital Council of Southern California in a HealthLeaders Media article.[38] "Measurable savings will be realized as middleware is installed that will allow for the electronic transmission and translation of patient records across different proprietary systems between delivery networks. The savings for hospital-centric EMRs will balloon when integration of these confined systems with the rest of healthcare delivery system is realized. The ideal circumstance would be the use of EMR smart cards that would be updated with every patient encounter and that can be read electronically by every medical provider treating the patient, regardless of the provider's medical network or health plan affiliation."

Other healthcare leaders appear to concur with Lott's sentiments. Paul Contino, former Vice President of Information Technology at Mount Sinai Medical Center, member and former chair of the Smart Card Alliance Healthcare Council, and Board Member of the New York Clinical Information Exchange (NYCLIX), states that he believes there is a huge potential for savings in many areas with integration of smart cards into the healthcare information tapestry.

To emphasize the point, Contino cited an exhaustive analysis of one hospital's medical records that resulted in the discovery of 200,000 duplicate records. Fixing those problems costs between $60 and $100 each. "That's $1.5 million in medical record clean-up costs, and you have the problem again every two or three years because of registration mistakes. You can avoid this cost with smart cards," said Contino.[39]

[38] "Four Health Leaders Weigh in on Whether EMRs Save Money," *HealthLeaders Media*, November 24, 2009, http://www.healthleadersmedia.com/content/TEC-242577/Four-Health-Leaders-Weigh-in-on-Whether-EMRs-Save-Money

[39] "Power to the Patient: Mount Sinai Puts Medical Records Snapshot on Smart Cards," *CIO*, October 16, 2007, http://www.cio.com/article/146750/Power_to_the_Patient_Mount_Sinai_Puts_Medical_Records_Snapshot_on_Smart_Cards

6.1 Are Funds Available for Implementing Smart Cards?

With publication of the "Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology; Final Rule,"[40] CMS officially put into place the steps for providing incentive funds for the adoption of certified healthcare technologies that support the goals of the HITECH Act and enable providers and hospitals to demonstrate meaningful use of those healthcare technologies. Healthcare provider investment in technologies such as smart cards will be offset by incentive funds that equate to tens of thousands of dollars each for eligible providers and between $4-6 million, on average, for each hospital. Certain hospitals will receive direct reimbursement of up to 75% for any directly related EHR technology adoption and utilization expense.

According to a July, 2010, CMS press release, "The HITECH Act supports the adoption of electronic health records by providing financial incentives under Medicare and Medicaid to hospitals and eligible professionals who implement and demonstrate 'meaningful use' of certified EHR technology. The CMS regulations announced today specify the objectives that providers must achieve in payment years 2011 and 2012 to qualify for incentive payments; the ONC regulations specify the technical capabilities that EHR technology must have to be certified and to support providers in achieving the 'meaningful use' objectives."[41]

This announcement contains three key points: 1) the HITECH Act supports the adoption of electronic health records by providing financial incentives; 2) providers (and hospitals) must achieve specific meaningful use objectives (by no later than 90 days prior to submission of an application) in order to qualify for incentive funds; and 3) EHR technologies must have specific technical capabilities in order to be certified and support healthcare providers in this process. (The provider or hospital only receives funds for implementing certified technologies.)

The major challenge ahead for all healthcare technology vendors who wish to continue to provide hardware, software or services to enable and support meaningful use is becoming certified. The first round of applications for certification has been filed, and although as of August 2010, no "certified EHRs" existed under the current regulations, several technology vendors continue to move forward with preparing to demonstrate the new functionality, testing, interoperability and security requirements required to achieve eventual certification. Until that time, healthcare facilities and providers must continue implement available technology, to maximize their potential to receive incentives in the first distribution round from October 2010 to October 2011.

[40] http://edocket.access.gpo.gov/2010/pdf/2010-17210.pdf
[41] http://www.hhs.gov/news/press/2010pres/07/20100713a.html

7 Summary

The Smart Card Alliance believes that smart card technology and smart card-based systems meet a number of criteria for meaningful use:

- Smart cards augment the security of EMRs/EHRs by providing strong authentication which corresponds to at least Level 3 Assurance of the OMB's 04-04 Memorandum.
- Smart cards can carry PKI certificates which provide the highest level of trust identity management for data interchange across networks.
- Federal standards are in place for identity verification and data access and security which use smart cards (the FIPS 201 Personal Identity Verification (PIV) standard for Federal employee and contractor identification cards).
- Smart card software is commercially available that can improve the quality, safety and efficiency of healthcare delivery while improving care coordination and data access.
- Smart card technology can help institutions manage a qualified EHR by integrating information from other external sources.
- Smart card technology honors the goals of certification criteria by: promoting interoperability, promoting technical innovation which embrace adopted standards, keeping implementation costs low, considering best practices, and providing a modular solution.

As the industry moves forward in the pursuit of meaningful use in EHR implementation, standard best practices will include sharing data from various media across multiple networks. For information to be useful, it must be accurate, secure, and related to a single individual. Access to sensitive medical information must only be granted to known (authenticated) individuals or institutions that can supply valid identity credentials and that are authorized to access the information. Information must be able to be updated and must be synchronized across all networks in real-time. Individuals or entities that access, document and modify medical information (e.g., by adding to a medical record) must provide credentials to demonstrate that the resulting data can be trusted and is accurate. Finally, confidence in the technology, by the healthcare industry, providers and facilities, and consumers, is a requirement for success. Smart card technology can be used to address all of these requirements, with a long history of global success that can help build confidence in the new healthcare systems.

Smart card technology can augment existing EMR/EHR systems to provide the critical functionality necessary to achieve meaningful use, as well as to address important security and privacy gaps that could compromise the future use and utility of emerging regional and national health information networks.

8 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Healthcare Council to discuss the ways in which smart card technology and smart card-based systems can better position healthcare organizations for meaningful use of electronic health records, while addressing many of the security and privacy challenges that come with electronic health records and health data exchange.

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 thanks the Council members for their contributions. Participants involved in the development of this white paper included: Computer Sciences Corp. (CSC); Gemalto; Giesecke & Devrient; IBM; IDmachines; LifeMed, Inc; MasterCard Worldwide; Mount Sinai Medical Center; Northrop Grumman Corporation; Oberthur Technologies; OTI America; SCM Microsystems; XTec, Inc.

Special thanks go to **Rachelle Blake and Dale Grogan**, LifeMed, Inc., who contributed the first draft of the white paper. Healthcare Council members who participated in the development and review of the white paper included:

- **David Batchelor**, LifeMed, Inc.
- **Rachelle Blake**, LifeMed, Inc.
- **Gary Christoph**, Northrop Grumman Corp.
- **Paul Contino**, Mount Sinai Medical Center
- **Sal D'Agostino**, IDmachines
- **Anna Fernezian**, CSC
- **Dale Grogan**, LifeMed, Inc.
- **David Hemsath**, IBM
- **Rick Lazerick,** CSC
- **Michael Magrath**, Gemalto
- **Ola Martins,** Oberthur Technologies
- **Cathy Medich**, Smart Card Alliance
- **Bob Merkert**, SCM Microsystems
- **Matthew Neuman**, Giesecke & Devrient
- **Curt Palmer**, MasterCard Worldwide
- **Rick Pratt**, XTec, Inc.
- **John Rego**, OTI America

About the Smart Card Alliance Healthcare Council

The Smart Card Alliance Healthcare Council brings together payers, providers, and technologists to promote the adoption of smart cards in U.S. healthcare organizations. The Healthcare Council provides a forum where all stakeholders can collaborate to educate the market on how smart cards can be used and to work on issues inhibiting the industry. Healthcare Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects.