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

A Smart Card Alliance Report

Publication Date: September 2003

Publication Number: ID-03004

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

About the Smart Card Alliance

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

Table of Contents

Executive Summary

HIPAA Creates a Need for Secure, Protected Health Care Information

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) affects health care organizations in two ways: first, by strongly encouraging the conversion of paper-based health care information systems to electronic systems, and second, by mandating that the design and implementation of the electronic systems guarantee the privacy and security of patient information gathered as part of providing health care. To achieve HIPAA compliance, health care organizations must implement physical, technical, and administrative safeguards that ensure the integrity and security of health care information.

Multiple Technologies Are Used to Meet HIPAA Requirements

Historical requirements for protecting facility access mean that multiple techniques are candidates for fulfilling the HIPAA requirement to safeguard information physically. The rise of the Internet has led to the development and use of numerous technologies, such as firewalls, smart cards, virtual private networks (VPNs), public key cryptography, and other standards-based[1] encryption technologies that can satisfy the requirement to safeguard electronic information. An appropriate safeguard must also support the provision of fast, efficient, and appropriate medical care and allow institutions to meet their need to track patients, verify patient eligibility, and bill appropriate entities for appropriate amounts. Additional considerations include concern for the patient experience and the experience of the health care provider, for whom the system is a secondary consideration and ease of use is critical.

Smart Cards Represent an Excellent Solution for HIPAA Compliance and Support New Applications That Improve Medical Care

The presence of processing capability and memory in a smart card, along with the smart card's ability to support multiple applications, make smart cards an efficient and flexible mechanism that can help organizations achieve HIPAA compliance while meeting the goals of patients and practitioners. Smart cards have a unique ability to make information access easier for users while at the same time enforcing the more robust security policies required of health care organizations to bring their environments into HIPAA compliance. Smart cards can represent an excellent solution to an organization's multiple physical and electronic security requirements.

Systems that use smart cards as the identity token and secure data carrier have unique benefits.

- Smart cards can provide easier information access management, ensuring that users are following established security policies.
- Smart cards are a familiar form factor that can be used for both physical access to facilities and logical access to information on personal computers and networks.

[1] For example, American National Standards Institute (ANSI) and Federal Information Processing Standards (FIPS).

- Smart cards can help enforce access control to health information, providing support for both user authentication and encryption of data on the card and during transmission.
- Smart cards can store health information on the card, performing as secure portable data carriers that are under the control of the patient and the health care professional.
- Smart cards, with on-card intelligence and processing capabilities and the ability to use standards-based cryptography, are uniquely capable of enabling compliance with strong privacy guidelines and of enforcing the privacy and security policies set by the health care organization.
- Smart cards provide a feature-rich platform for health care organizations to implement new applications that improve access to and convenience of medical care.

Health care organizations worldwide are implementing smart health cards. With the appropriate security architecture, smart cards can be a very valuable tool to providers, insurers, and patients alike. In addition to being an instrumental component of a system that is designed to ensure compliance with HIPAA regulations, smart cards can also support new applications that deliver clinical and administrative benefits.

About This Report

This report was developed by the Smart Card Alliance to describe how smart cards can be used to meet HIPAA Security Rule and Privacy Rule requirements. Designed as an educational overview for decision makers, it summarizes the HIPAA privacy and security requirements, provides an overview on how smart cards work, describes how smart cards can be used to support HIPAA compliance and implement other health care applications, and outlines key implementation success factors. The report also includes profiles of smart health card implementations including the University of Pittsburgh Medical Center, Mississippi Baptist Health Systems, and the French, German and Taiwanese health cards.

This report provides answers to commonly asked questions about the use of smart cards as health care cards, such as:

- What requirements do the HIPAA Security Rule and Privacy Rule impose on health care providers, insurers, and patients?
- How do smart cards work?
- How can smart cards help health care organizations fulfill the HIPAA requirements?
- What capabilities do smart cards provide for clinical and administrative benefits that extend beyond HIPAA requirements?
- What can we learn from organizations who are currently using smart cards as health care cards?
- What considerations are important to the successful implementation of a system that uses smart cards as health care cards?

HIPAA Privacy and Security Requirements

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) has two goals:

- To protect health insurance coverage for workers and their families.
- To encourage the development of a health information system by establishing standards and requirements for the secure electronic transmission of certain health information.

The term HIPAA refers not only to the original law but also to a set of standards and regulations passed later to implement the law. These standards and regulations cover privacy, security, electronic transactions, simplification of procedures, and enforcement procedures[2] that are intended to promote and safeguard the electronic transmission of health-related data. They comprise a national standard for electronic health care transactions, including uniform code sets,[3] unique identifiers for providers, employers, plans, and individuals, and regulations governing the privacy, confidentiality and security of any information that is collected in connection with providing health care services. HIPAA therefore applies to the protection of electronically maintained and transmitted health care information.

HIPAA Objectives

To achieve the goals stated in the Act, HIPAA has two main objectives:

- Make health insurance portable.
- Simplify the administration of health care information.

Insurance portability allows people changing jobs to transfer their health insurance information in a standard way, thereby ensuring coverage at their new jobs. Simplified administration reduces administrative costs and standardizes the exchange of health care information, while ensuring that patient confidentiality is protected.

The HIPAA administrative simplification provisions include a minimum set of privacy and security standards to protect "individually identifiable" medical information.[4] These standards are two major elements of the HIPAA regulations.

The privacy standards (collectively called the Privacy Rule) define what is meant by appropriate access and define who has access to what kinds of information. These standards also protect the confidentiality of data once someone has been granted access. The requirements of the Privacy Rule

[2] Joseph Goedert, "HIPAA's Long and Winding Road," *Health Data Management*, March 7, 2003.

[3] Code set means any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes.

[4] Individually identifiable health information is any information, including demographic information, collected from an individual, that is created or received by a health care provider, health plan, employer, or health care clearinghouse, and that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and that either identifies the individual or can reasonably be assumed to be used to identify the individual.

apply to anyone who creates or maintains individually identifiable health information. The Privacy Rule has its own security requirements that require all health care providers to safeguard protected health information from any use or disclosure that violates the Privacy Rule, intentionally or unintentionally.

The security standards (collectively called the Security Rule) describe how to ensure the privacy and confidentiality of information.

The administration simplification provisions therefore mandate that health care providers provide physical, technical, and administrative safeguards to ensure the integrity, security, and confidentiality of health information in every form — electronic or on paper.

HIPAA Compliance Schedule

The original Act became law in 1996. The standards developed to implement the Act were developed at different times and have different compliance schedules.[5] Figure 1 lists the dates by which the entities to which HIPAA applies must comply with several of the standards included in HIPAA. In addition, standards for a health care provider identifier, national health plan (payer) identifier, claims attachments and enforcement procedures are also being defined.

Figure 1: Compliance Dates for Standards Included in HIPAA

Standard	Compliance Date	Applies to Organizations
Electronic health care transaction and code sets	October 2003	All covered entities
Privacy Rule	April 2003 April 2004	All covered entities except small health plans Small health plans
National employer identifier	July 2004 July 2005	Large organizations Small organizations
Security Rule	April 2005 April 2006	All covered entities except small health plans Small health plans

Privacy Rule

The HIPAA Privacy Rule creates national standards to protect individuals' medical records and other personal health information. The rule became effective on April 14, 2001. Most health plans and health care providers covered by the new rule had to comply with its requirements by April 2003.

[5] Joseph Goedert, "HIPAA's Long and Winding Road," *Health Data Management*, March 7, 2003.

The Privacy Rule achieves the following:

- It gives patients more control over their health information.
- It sets boundaries on the use and release of health records.
- It defines appropriate safeguards that health care providers and others must establish to protect the privacy of health information.
- It holds those who violate patients' privacy rights accountable, establishing both civil and criminal penalties for violations.
- It strikes a balance between privacy and public responsibility when disclosure of data is required, such as to protect public health.

For patients, the Privacy Rule means being able to make informed choices, based on how personal health information can be used, when seeking health care or reimbursement for health care. The Privacy Rule provides patients with information about whether and how their information can be disclosed to third parties, what limitations are on allowable disclosure, and what their rights are for obtaining their own health care records.[6]

Security Rule

The HIPAA Security Rule requirements apply to health plans, health care clearinghouses, and health care providers. The Rule covers all health information about an individual that is electronically collected, maintained, used, or transmitted.[7] The final Rule was published on February 20, 2003.

The Security Rule includes three groups of security standards, all intended to protect data integrity, confidentiality, and availability:

- Administrative safeguards.
- Physical safeguards.
- Technical safeguards.

The standards governing administrative safeguards document formal practices to manage the selection and execution of security measures and to define how personnel are required to act to protect data.

The physical safeguard standards protect physical computer systems and buildings from fire, intrusion and other environmental hazards. They also control access to such facilities, describing the appropriate use of locks, keys, and administrative access control measures.

The technical safeguard standards include processes to protect, control, and monitor information access.

An important part of the safeguards is the ability to uniquely identify the user who is logging on to the system, to authenticate this person (allowing for role-based security level identification), and to authenticate the electronic health information integrity.

HIPAA also includes an electronic health care transaction and treatment code sets rule. This rule defines the transaction sets that standardize electronic transactions required to ensure confidentiality and security of

[6] U.S. Department of Health and Human Services, Office for Civil Rights, *Standards for Privacy of Individually Identifiable Health Information*, [45 CFR Parts 160 and 164].

[7] U.S. Department of Health and Human Services, Office for Civil Rights, *Standards for Privacy of Individually Identifiable Health Information,* [45 CFR Part 142 – Security and Electronic Signature Standards].

health information.[8] The use of these standard transactions and code sets is intended to simplify administration and enable the efficient electronic transmission of certain health information. The rule also contains requirements concerning the use of these standards by health plans, health care clearinghouses, and certain health care providers.

Current Implementations

As Figure 1 indicates, large health care organizations were required to comply with the HIPAA Privacy Rule by April 2003. The Privacy Rule includes certain security requirements, since data cannot be kept private without security. When the Security Rule becomes law in 2004, additional measures may be required.

Currently, systems that meet the Privacy Rule requirements do so using new processes and procedures, as well as a number of different technologies. The majority of these systems use firewalls and virtual private network (VPN) implementations for security. Some systems include a public key infrastructure (PKI) and incorporate user ID-password logons.[9] Smart cards are being used in new health care system implementations, with many organizations considering the use of both smart cards and biometrics.

Figure 2 summarizes how these different technologies operate to improve the security and privacy of an information system.

[8] Goedert, op. cit.

[9] For example, The Centers for Medicare and Medicaid Services (CMS) have implemented many such solutions and list the preferred CMS processes on their website, http://www.cms.hhs.gov/it/roadmap/standards/TRM.pdf.

Figure 2: Technologies Used to Improve Information System Security and Privacy

Technology	Usage
Firewalls	Firewalls prevent unauthorized access to a private network that is connected to the Internet or another public network. A firewall filters the data traffic that flows between the two networks. The firewall prevents unknown external sources from accessing data on the internal network. In addition, firewalls can prevent viruses from being implanted in an internal network.
Virtual Private Networks	VPN is the term used to describe a private network that is constructed between two nodes using public wires. A VPN establishes trust between the interconnected nodes. All communications are encrypted, and each node knows what encryption is used. A VPN requires special hardware and software and is therefore difficult and expensive to implement. Also, a VPN can only protect a one-to-one connection.
Public Key Infrastructure[10]	A PKI is a system of digital certificates, certificate authorities, and other registration authorities that verify and authenticate the validity of each party involved in an online transaction. PKI relies on public key cryptography, in which a so-called "key pair" is used to encrypt and decrypt messages sent electronically over unsecured paths. The two keys in a key pair are complementary mathematical algorithms. When one key performs a certain function (such as encrypting an electronic message), only the other key in the pair can perform the complementary function (decrypting the message), thereby authenticating the sender and validating the message integrity. Knowledge of one key (the public key) does not require knowledge of the other key (the private key), which is held in confidence by its owner. PKI protects electronic messages sent over unsecured paths. Using PKI can satisfy the HIPAA requirements for data confidentiality, user authentication, access control, data integrity, and support for non-repudiation of data. Using PKI can also satisfy other HIPAA requirements for certain administrative procedures, physical safeguards, and audit trails.
Smart Cards	A smart card is a plastic card with an embedded chip that can be either a microcontroller with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless electromagnetic interface. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signatures) and interact intelligently with a smart card reader. Smart cards are used worldwide in financial, telecommunications, transit, health care, secure identification and other applications.
Biometric Technologies	Biometric technologies authenticate an individual by validating one of the person's physiological features, such as a fingerprint, iris, face or voice. The physiological feature can be captured and stored as a full biometric image or as a template.[11] Biometric information can be stored on a card or in a host computer. Using biometrics, an individual can be identified locally (for example, by comparing a physical fingerprint with a fingerprint template saved on a card) or remotely (by comparing the physical fingerprint with a fingerprint template saved on a host computer).

[10] A good PKI reference book is *Planning for PKI*, by Russ Hously and Tim Polk, John Wiley & Sons, March 13, 2001.

[11] A template is a unique representation of the biometric of the authorized cardholder (e.g., fingerprint, iris) that was created using a mathematical algorithm on the original biometric image. Templates are typically more compact than full biometric images, requiring less storage, and cannot be reverse-engineered to re-create the full biometric image.

Overview of Smart Cards

Historical Background

A smart card is a plastic card in which an integrated circuit, or chip, is embedded. Systems using smart cards have multiple point-of-service terminals (or readers) which communicate with the card and with a central host computer system. The development of smart cards dates back to the 1970s, when patents were filed in France, Germany, and Japan.

The first practical smart card implementation was developed in France, to combat the rising cost of fraud in telecommunications and banking applications. Motorola produced the first secure single-chip microcontroller (MCU)[12] in 1979 for use in French bank cards. Two types of smart card products were introduced in the early 1980s. One, for telephone cards, used a serial-memory integrated circuit (IC)[13]. The other, for banking applications, used the more secure MCU.

The first mass rollout of smart cards took place in 1992, when the cards were adopted by all French banks. More than 10 million cards were issued that year. MCU smart cards shipments have grown dramatically, with 727 million shipped in 2002[14] and over 1 billion expected to ship annually within the next 2 to 3 years. This rapid growth is due to the increasing use of smart cards for many financial, telecommunications, transit, health care and secure identification applications.

What started as an electronic device to store bank account information securely has evolved into a sophisticated computing device capable of supporting many different applications on a single card or token. These applications include bank cards, mobile phone subscriber identity modules (SIM), health cards, government and enterprise ID cards, benefits and social welfare cards, driver's licenses, physical and logical access cards, mass transit (ticketing) cards, and even cards that combine multiple applications on a single card.

Components of a Smart Card

It is the interactive and decision-making capabilities of the dedicated microcontroller embedded in the card that distinguishes a smart card from other identity token technologies. The MCU includes the following components:

- A CPU for managing data, executing cryptographic algorithms and enforcing application rules.

[12] An MCU is a computer chip that contains the components of a controller. Typically, these include a central processing unit (CPU), random access memory (RAM), some form of read-only memory (ROM), electrically erasable programmable read-only memory (EEPROM), input/output (I/O) ports, and timers. Unlike a general purpose computer, a microcontroller is designed to control only a particular system

[13] A memory-only smart card chip contains a memory array with hard-wired security logic to control access to the memory and to prevent unauthorized writing and erasing of the data. It has neither a microprocessor nor MCU, so its functionality and security capabilities are limited.

[14] Dataquest: Worldwide Chip Card and Semiconductor Vendor Market Share, 2002 *Focus Report*, 24 April 2003.

- ROM for storing operating system (OS) software. Some vendors offer flash EEPROM[15] as an option to ROM.
- RAM for temporary storage of data.
- Electrically erasable programmable read-only memory (EEPROM) for storing variable data, such as cardholder information, passwords, and transaction details.
- Card OS software for controlling one or more applications.
- Application software, dedicated to one application or supporting multiple applications.
- Dedicated hardware security features that prevent access to software and data stored in memory from physical or logical attacks.
- Optional additional processors for rapid encryption functions.

Two important components of the MCU-based smart card are the application software and the OS. The application software implements all applications supported by the smart card. Smart cards can be dedicated to one specific application or support multiple applications. Regardless, all applications are controlled by the smart card's OS.

Some cards run a so-called "native" OS, which is tightly integrated with the installed applications. Others run an open OS (such as Java Card or MULTOS). In these cards, the applications are separated from the OS by an application program interface (API), allowing the applications to be developed independently from the OS. The OS ensures the overall security of such a system by using "firewalls" to separate the applications internally from each other and from the OS.[16]

In addition to loading, operating, and managing applications, a smart card's OS handles the following functions:

- Data transmission over a bidirectional, serial terminal interface.
- Execution control and instruction processing.
- Protection of access to data.
- Memory management.
- File management.
- Management and execution of cryptographic algorithms.

A simplified smart card manufacturing process is illustrated in Figure 3.

[15] Flash EEPROM memory, like EEPROM, can be reprogrammed but can be locked to function as ROM. This provides flexibility for rapid software development and fast time-to-market by avoiding the need for custom mask manufacturing for the smart card chip.

[16] The liability of the provider of the OS can also be mitigated by the use of application owner-controlled cryptography, as described in ANSI standard X9.69. This affords the application owner cryptographic isolation from the card itself, as well as distinct separation between applications.

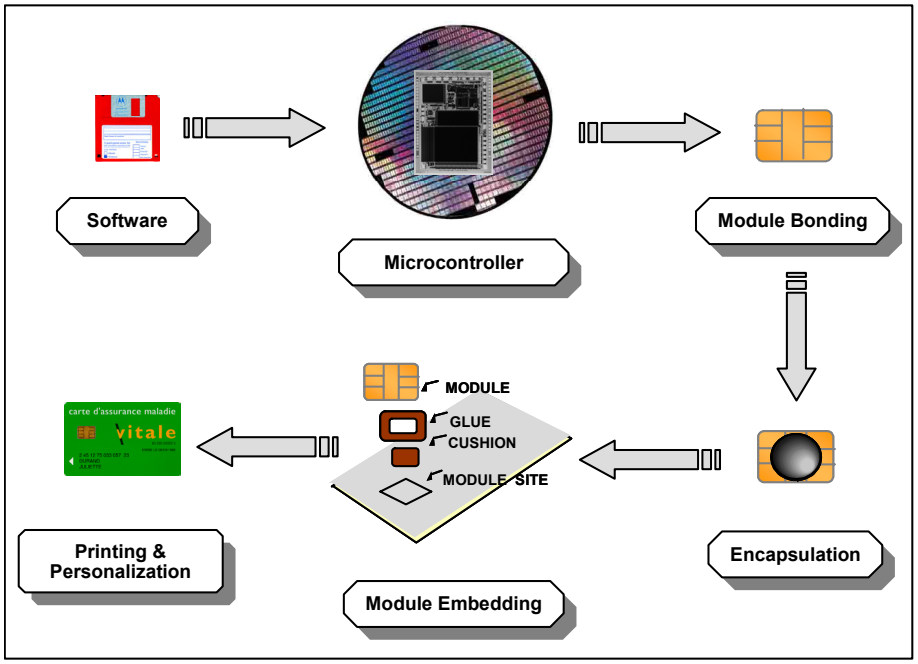


Figure 3: Smart Card Manufacturing Process

Major Advantages of Smart Cards

The evolution of smart cards has often been referred to as being analogous to the evolution of the personal computer (PC). In fact, the computing power of the average smart card today is greater than that of the PCs introduced in the early 1980s. And as happened with the PC, there has been a continuous demand for smart cards with additional memory and more efficient software.

This demand is driven by the advantages the smart card offers over the conventional plastic card with a magnetic stripe. The magnetic stripe card, which was introduced in the early 1970s and is familiar as a credit card or loyalty program card, has four significant drawbacks.

- Vulnerability to fraud.
- Limited capacity for application data storage.
- Non-interactive transaction processing capabilities.
- Limited application support.

Robust Security

Magnetic stripe cards are more vulnerable to fraud than smart cards. It is relatively easy to replicate either the data on a magnetic stripe card, or the card itself, using equipment that can cost as little as $25. This vulnerability has led to an increase in both financial fraud and identity theft worldwide.

Memory IC smart cards store authentication information in the chip. In their most secure form, memory cards store a unique serial number and include the ability to lock sections of memory permanently or allow write access only by using password-protected mechanisms. In general, memory cards employ no additional security to protect their contents; however, a few

vendors now offer devices with encryption capability. System-level methods can also be used to encrypt and decrypt the information stored on the card.

MCU smart cards can take security one step further. Such smart cards can implement authentication or standards-based encryption methods in software or firmware. The embedded MCU gives the cards more sophisticated security capabilities, such as the ability to perform their own on-card security functions (e.g., encryption, hardware- and software-based tamper resistance features that protect card contents, and digital signatures) and interact intelligently with the card reader.

Increased Storage Capacity

The conventional magnetic stripe card has a limited storage capacity of around 200 to 400 bytes of memory. A memory smart card typically has 2 to 4 kilobytes (KB) of memory. MCU smart cards are being introduced today with over 300 KB of memory. This larger amount of memory accommodates more applications or data (or both) on the card, more sophisticated software and encryption for additional security and, with appropriate system design, better privacy protection for the cardholder. The additional memory capacity can permit the secure storage of biometric data, such as a fingerprint, iris, or facial recognition pattern, providing additional security and identification features.

Smart cards are now available with radio frequency (RF) contactless interfaces. Such cards do not have to be inserted into a card reader but are merely waved close to it, thus providing greater user convenience, faster throughput, and fewer mechanical failures.

Flexibility and Intelligence in Transaction Processing

The term “smart card” derives from the presence of the chip embedded in the card. The chip supports interactivity and enables the card to make decisions during transactions. The card can therefore react differently, depending on what information it receives.

Support for Multiple Applications and Multiple Functions

One major advantage of smart cards over magnetic stripe cards is the ability of a single smart card to support multiple applications. However, this ability can raise concerns about the security and privacy of data on the card.

For a card to support multiple applications, the applications must be truly independent of one another. This means that one application must not be able to overwrite another’s data or have access to another’s data without that application’s permission. When an application is running, it must not affect the operation of any of the others on the card in any way. The same is true when an application is being loaded or deleted.

Truly separate applications can be achieved by proper design. Key are memory management and the appropriate, controlled use of cryptographic techniques. Defined blocks of memory must be allocated to each application and controlled by the OS. Proper memory management requires an authorization process in which each application is authorized to run or to access RAM and EEPROM memory. The OS must also provide each application with the means for user authentication as part of application authorization. The control of the cryptographic process by the application owner also isolates the issuer of the card and its OS from the application.

A single application installed on a smart card can sometimes support multiple functions (for example, a banking application may have a credit function, a debit function, a loyalty function, and perhaps an electronic purse). Each function is managed and trusted by the application. When a card supports a single such application, it is referred to as a multi-function card.

A multi-function card does not require a multi-application OS, even if some of the functions are inactive when the card is issued. However, if the card will be required to support truly independent applications (applications that are developed independently and without complete trust in each other), a multi-application card is required. The operating system and the applications must be separated by an API and by the appropriate use of cryptographic techniques. Applications can then be loaded onto the card independently and without requiring knowledge of each other.

The appropriate choice of card, operating system, cryptography, and chip depends on what the smart card is expected to do. Independent smart card laboratories, accredited by governments, can verify and assess that the product performs appropriately.

How Smart Card Transactions Work

Smart card transactions involve communication between the card, a card reader or terminal, and other systems (such as a host computer) on a network with which the card reader can communicate. All communications to and from the smart card are carried out using a module contact plate on the surface of the card, which is connected to the bi-directional I/O port on the chip. Only the card or the reader can communicate at one time.

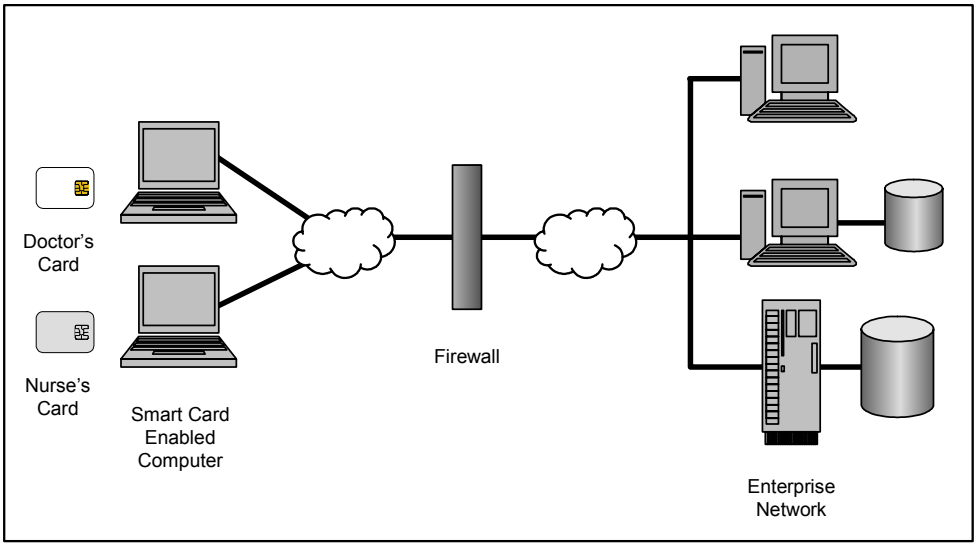
A transaction begins when the smart card reader initiates communication with the card. The routine is always based on the so-called request-response procedure. The reader sends a request (an instruction), the card processes the request and sends a response, and a dialog follows between the card and the reader. A series of instructions to the card trigger card actions, such as read or write instructions relating to files stored in the chip that contain data or authorizations or both. This type of request-response activity is carried out between the reader and the card regardless of the application. It does not matter whether the transaction requests authorization for payment or access to a physical site or a logical site such as a computer file.

To understand how a system could work in practical terms, consider an example application where a smart card is used to provide access to networked resources and data (see Figure 4).

- The user inserts the smart card into the smart card reader connected to a laptop or other computer.
- The user typically “unlocks” the card with a PIN or password. The system (either the laptop or the host system depending on the system design) authenticates that the inserted card is a valid card and reads authentication information from the card (as described above).
- The authentication information is securely communicated via the network to the networked enterprise system. Either an authentication server or an application receives the data, determines the user’s privileges and provides access only to those resources that the cardholder is authorized to access. For example, the smart card used by a doctor can provide full read/write access to

information, while a smart card used by a nurse could provide more limited access.

Figure 4: Smart Cards Used for Logical Access



Smart Cards in Health Care: Supporting HIPAA Compliance

Data Use in the Health Care Environment

As more and more protected health care information is stored or transmitted electronically and becomes network accessible, health care organizations have become increasingly concerned with controlling access to that information. HIPAA requires all health care organizations that create or maintain electronic health care information to secure the information from any use or disclosure, intentional or unintentional, that violates the HIPAA Privacy Rules.

The use of electronic medical records offers many benefits to organizations throughout the health care industry, including lowering administrative costs, reducing errors, and improving an organization's ability to measure and improve the quality of care. As a result, health care organizations are investing heavily in information technology each year. Access to patient data has expanded well beyond users in the organizations that gather the data to begin with.

The way health care is delivered today, through managed care groups, has also accelerated the demand for electronic health care data and changed the way information is accessed and shared. Integrated delivery systems (IDSs) consolidate data from various providers (such as hospitals, clinics, and in many cases, health plans) under one umbrella, providing multiple access points to the same data. Information is then shared among the different organizations that are members of the IDS. Health maintenance organizations (HMOs), which are often part of a larger IDS, rely on analysis of aggregated patient data to determine optimal care practices and measure costs for various treatments and services. Third-party accreditation organizations collect data on treatment and care of patients to develop quality reports for industry use. Pharmaceutical and medical device companies analyze patient data to improve their product offerings and remain competitive. Research laboratories analyze data in a clinical setting to determine the effectiveness of diagnostic tests and treatment methods.

To illustrate how health care data is accessed and used by various individuals and organizations in a managed care setting, consider a very large regional health care organization. Such an organization typically is composed of hospitals, clinics, physicians, caregivers, and a multitude of available health plans.

Over 60% of the data users within such an organization are part of the care delivery system. Those who have access to electronic patient data include physicians, nurses, and administrative personnel. Such a system typically also has HIPAA-defined business associates, such as paramedic services, who need access to patient data to bill their services. The health plan, or insurance, segment of such a system accesses patient data to process payments for care. In most instances, the patient's medical record itself need not be accessed – just the patient's ID number and the HIPAA code sets assigned to the treatment that the patient received. There are times when special treatment of a patient requires further investigation of a medical record by an insurance company to determine level of coverage.

Data transfer and access between organizations for claims purposes are typically accomplished within a closed electronic data interchange (EDI) network. But an EDI network can only be accessed by those within the managed care system and is relatively expensive for small offices or

independent health care providers. Managed care systems might therefore employ health care clearinghouses to process data and claims from supported care groups that are not part of the primary care system. Clearinghouse personnel require secure, controlled, remote access to patient records to process claims. Most health care organizations today have implemented some type of VPN system to support secure remote access, with additional role-based access control mechanisms to assure appropriate "right to know" controls. User authentication is most often accomplished with a user ID and password combination, but in some instances, one-time password tokens are used to strengthen the authentication process.

Caregivers are the most demanding data users in a health care organization. They are also the most challenging to support from the perspective of information technology. This challenge will only become stronger as the use of electronic medical records increases and more health care organizations implement computerized physician order entry (CPOE) systems. A physician might require access to 20 or more applications to obtain the data needed to treat a patient or complete an order entry. The physician may be accessing the system locally, from a primary hospital or clinic, or remotely, from an out-of-network hospital or clinic. Accessing a system remotely can be accomplished using a token device to identify and authenticate the physician to the network and by providing the appropriate permissions to access information; once on the network, however, the physician may still need to remember multiple passwords to access all required applications.

Currently, some health care organizations feel that establishing a strong password policy is enough to satisfy HIPAA security requirements. But if a caregiver is forced to remember 20 passwords over the course of a day, convenience and the need for access may surpass the caregiver's attention to security policy. There are many ways for users to bypass security controls for convenience, including sharing passwords with colleagues, writing passwords down, using easy-to-remember passwords (which are also easy for unauthorized personnel to guess), and reusing the same password multiple times. Security controls will be bypassed if a caregiver believes that health care will suffer from lack of access to important information.

In this environment, it is especially critical to balance the need to protect patient information with the need to access that information efficiently and ensure quality care.

Advantages of Smart Cards in the Health Care Environment

HIPAA requirements mandate that storage of and access to health care information fulfill the following requirements:

- Availability. Data must be accessible and usable upon demand by an authorized entity.
- Integrity. Data must not be altered or destroyed in an unauthorized manner.
- Confidentiality. Data cannot be made available or disclosed to unauthorized individuals, entities, or processes.

Smart card technology can help organizations meet these requirements, along with additional requirements imposed by the need to protect electronic information.

Enforcement of Security Policies

One of the biggest challenges for electronic information access management and control is ensuring that users follow security policies established to protect such information. Health care organizations are populated by users for whom the requirement to remember multiple passwords may be a distraction. As a result, users either circumvent the organization's security policy or are not able to access critical data.

A smart card can store multiple passwords and access credentials. To access data, users simply insert the card in a card reader at a computer and provide the required verification information. Users take the same action each time, regardless of whether they are accessing a computer, a network, an application, or a Web site. Users also take the same action regardless of the verification method used, be it a password, digital certificate, dynamic password, or biometric. System administrators benefit by being able to enforce stronger security policies and employ a mix of credential types in their environment without forcing a change in the user experience.

Integration with Existing Facility Access Control

A single smart card can include multiple technologies to support requirements for facility access control. If an organization already requires the use of a card for facility access, there is minimal adjustment for the user, who will already be familiar with the credential. An individual's picture can be printed on a smart card, visually validating the person's right to access an area or facility. A single card can also support different electronic controls, such as magnetic stripe and barcode applications or proximity or biometric based controls.

Support for Information Availability, Integrity, and Confidentiality

A smart card is the ideal technology for enforcing access controls and protecting information while making it simpler for authorized users to gain access and store or retrieve information. The user must "unlock" the smart card once only (with a PIN or a password). The smart card then, using multiple technologies, enforces all required controls.

Unique Identifier. The unique identifier assigned to a user can be securely stored on a smart card. Because the identifier is stored on the smart card and not on a computer, the identifier cannot be stolen or used by someone else without the user's permission.

Encryption and Decryption. Standards-based encryption protects stored data and data in transit. Smart cards support various encryption technologies, including some of the strongest practical encryption algorithms such as Triple DES (Data Encryption Standard). Many available applications can provide smart card-based encryption and decryption of sensitive information, such as file, folder, and object-level encryption at a computer, email encryption, and VPN support. Encryption keys can be stored safely on a smart card and certificates can be generated on the card as needed, both for access and for encryption or decryption of stored data. The use of encryption keys can be combined with other technologies, such as PKI, to offer a convenient and secure method of managing private data.

Data Integrity. The use of a smart card combined with encryption and a digital signature is the strongest method currently available to verify that electronically protected information has not been altered or destroyed without

authorization. When an encrypted and digitally signed document is opened using a smart card, any alteration of the content is immediately recognizable.

User Authentication. Robust security requires user authentication techniques to validate a user's identity before the user can access protected information. Passwords provide weak authentication since they can be shared with others or stolen. However, smart cards combined with digital signatures or dynamic passwords can provide stronger two-factor authentication. The combination of something the user knows (a password or PIN) and something the user has (the smart card) provides a more reliable level of user authentication than a reusable password.

Biometric technology offers an alternative for strong user authentication. The combination of a biometric (as a replacement for a password or PIN) and a smart card can provide additional convenience for the user. The user needs only to insert the smart card and present the biometric, thus eliminating the requirement to remember anything. A biometric can also be used in conjunction with a smart card and a PIN or password to provide three-factor authentication (something the user knows, something the user has, and something the user is).

Transmission Security. Secure email and VPN technologies are two common ways of ensuring data integrity and data privacy. Most off-the-shelf email packages currently support the use of digital certificates for signing and encrypting email messages, and the use of role-based cryptography affords the persistent protection needed by the health care organization. Smart cards are a more secure vehicle for implementing digital signature technology, because they generate and store the public/private encryption keys and perform all cryptographic operations. The sensitive private keys are never released from the smart card chip.

Remote Access. Many health care organizations today are employing VPN technologies both for remote access to corporate networks and for shared access to data on protected Web sites (extranets). Multiple independent organizations, including health care providers accessing patient records and insurance companies processing claims, can leverage shared extranets by using VPN access.

A smart card protects a user's VPN credential (regardless of whether the credential is a password or a digital certificate) because the credential is permanently stored on the card. The credential is never exposed by being available in software or on the network. Among the major VPN vendors, digital certificates are becoming the primary credential for securing access to the network. When the digital certificate is stored on a smart card, an organization can verify and trust the identity of the person presenting the credential.

Smart cards also increase efficiency for VPN users. Users can access the network securely from anywhere, because their credentials travel with them on the smart card.

Support for Strong Privacy Policies[17]

Smart cards, with on-card intelligence and processing capabilities, are uniquely capable of enabling compliance with strong privacy guidelines and of enforcing the privacy and security policies set by the health care

[17] "Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology," Smart Card Alliance white paper, February 2003.

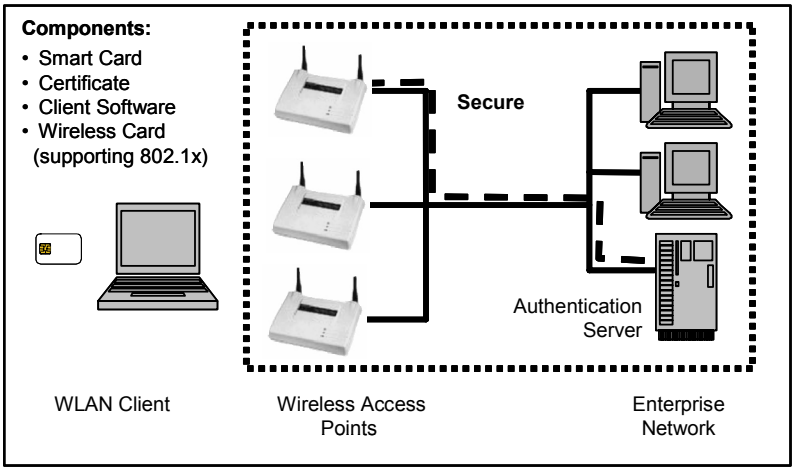
organization. Smart cards can protect personal information that is on the card, provide authenticated information access, and authenticate the legitimacy of other components during a transaction. When used appropriately and correctly, smart cards are the most privacy-protective of any ID card technology and provide unique features that both improve the system's security and protect the individual cardholder's privacy.

Securing Patient Information on a Wireless Network[18]

The mobile health care revolution is changing the way providers deliver care and how they access customer records. In order to quickly address patient needs and improve efficiency, health care organizations are using wireless networks in conjunction with laptop computers, handheld devices and PDAs, IP telephones, and tablet PCs. Patient information is streaming across unlicensed wireless radio frequencies. The protection provided by wireless device manufacturers, although enhanced in new wireless standards, is not enough to maintain the privacy of patient health information (or electronic health records).

Smart cards allow health care organizations to control access to wireless networks by providing strong, multi-factor authentication, supporting cryptographic protection for content, facilitating session key management, and allowing access only to authorized individuals. Additionally, smart cards allow mobility within health care organizations via seamless re-authentication and configuration management. By providing wireless users with a smart card, a PIN and the appropriate credentials to define access, employees, patients and partners can uniquely identify themselves when accessing networks or applications – even when users share a device.

Figure 5: Wireless Security with Smart Cards



[18] For more information on smart cards and wireless technology in health care, see the Mobile Healthcare Alliance at http://www.mohca.org and the WLAN Smart Card Consortium at http://www.wlansmartcard.org.

Use of Smart Cards as Health Cards: HIPAA and Beyond

The rise of smart card technology as a general purpose tool for security, identity verification, and transport of data has coincided with the national initiative to implement better privacy, security, and accountability for health care data. Smart cards clearly can be a useful tool for achieving these objectives, as well as for providing the security and access control features that are required by any enterprise. What is not as clear is how to design the security architecture and how the cards should be used.

Security Architecture

The architecture of a health care information system using smart cards leverages two features inherent in smart cards: flexible primary card functionality and multiple ways to protect data against unwarranted access. Together, these two features allow an organization to implement a solid security architecture.

Identifying Primary Card Function

Any proposed use of smart cards must first identify the primary function of the card. A smart card can function as a tiny database, securely carrying information relevant to the application in the on-card memory. It can also function as a highly secure passkey, providing access to electronic data stored in an online database (e.g., an "electronic vault"). These two functions are not necessarily exclusive; a card can be used both ways by the same application.

The card is valuable as a database because data stored on the card can be retrieved and used in environments where an online database is not available. Such retrieval requires only a small, inexpensive card reader with a display. However, the data that can be stored on the card is limited by the amount of card memory available. A full medical history, for example, which includes not only text data but also medical images, cannot be easily stored on any current-generation smart card.

Therefore, use of the card as a combination database and passkey is probably the best approach for health care applications. Small amounts of critical information can be stored on the card for use in offline situations, such as when an emergency medical technician (EMT) is trying to stabilize a patient before delivery to a hospital. The card can additionally be used as a passkey into online databases that can hold almost limitless quantities of data.

Unlocking Data

Regardless of where health care information is stored (on or off the card), principles of good security architecture and HIPAA compliance dictate that possession of the card not be enough to access the information. Because cards can be lost, loaned, or stolen, it is necessary to verify that the person holding the card is authorized to use it. Two basic technologies are recommended for authorizing access to health care applications: passwords and biometrics.

Use of passwords requires that the card be unable to divulge data or open an "electronic vault" unless the user supplies an appropriate password. This password can be unique to the card and should be known only to the card

and the cardholder. Multiple passwords can be used to unlock different card data and capabilities, although multiplying the number of passwords required tends to confuse and frustrate users and should be avoided if possible.

Use of biometric technology to determine whether the user is the authorized cardholder requires the measurement of some portion of the user's body (such as a fingerprint). A biometric is essentially a different kind of password, one that cannot be forgotten or replaced. Like all security technologies, biometric technology has specific strengths and weaknesses; user interface and security requirements should be considered when implementing biometric authentication.

Card Use by Providers

In the hands of health care providers, smart cards can assist with the fulfillment of HIPAA requirements for provider-based access control, including automatic logoff, audit trail generation, and data security.

Access Control

Smart cards can offer advantages for controlling both physical access (to buildings and other facilities) and logical access (to electronic information). Modern health care professionals, especially nursing staff, make heavy use of electronic records, and a major portion of the HIPAA compliance requirements are concerned with ensuring that provider-based access controls are applied to these records.

Smart cards can replace or augment systems that currently control physical access. In most situations, simple possession of a smart ID card is adequate verification of a person's right to be present in a hospital or clinic building or a sensitive area within such a building. When the card carries a printed image of the cardholder, other authorized personnel can help assure that lost or stolen cards are not being used to admit unauthorized personnel. Access to very sensitive areas may dictate the use of additional authorization to verify the cardholder's identity, such as a password or visual inspection by a guard or attendant at a controlled doorway. To control physical entry, it is recommended that the smart card execute a cryptographic challenge-response protocol with a doorway card reader. The additional time required is negligible, but the use of a cryptographic protocol makes successful card forgery extremely difficult.

Smart cards can also support fast, easy, and secure logical access. Like physical access, logical access should be implemented by executing a cryptographic authentication transaction between the card and the reader, as well as controlled role-based access to data. Unlike physical access, however, logical access should incorporate an additional verification step, requiring presentation of either a password or a biometric factor.

To protect logical access, HIPAA requires that an electronic session be terminated if it is inactive. Software can easily be programmed to terminate a session after a certain amount of time passes without any activity. A smart card can enforce this requirement automatically, invoking the software when the user removes the card from the reader. If the smart card is also used for physical access, the user is motivated to remove the card when the user moves away from the computer. Additionally smart cards allow the use of role-based security level identification. This means that a card issued and used by the physician has a higher level of access rights or permissions than the card issued to a nurse. A major HIPAA requirement is to not allow

access to those who do not need to see the information, while at the same time to make it easy for those who are allowed to get access quickly, securely and efficiently.

Audit Trail Generation and Transaction Accountability

HIPAA includes requirements for implementing mechanisms that record and support examination of activities in information systems that contain or use electronic health care information. The implementation method for auditing activities is to be determined by the health care entity, based on its risk management requirements.[19] In situations where data need to be secure and private, smart cards can allow audit information to be securely logged and reviewed.

Many situations also require formal authorization. For example, dispensing certain medications often requires a handwritten signature. As health care providers move away from paper processes to electronic ones, there will be a need to replace paper signature-based authorizations with electronic equivalents. Fortunately, digital signature technology provides an excellent solution. Digital signatures are fast and virtually impossible to forge.

Smart cards are an ideal mechanism for transporting and applying the cryptographic keys used to produce and verify digital signatures securely. However, some security precautions must be taken to prevent the use of lost, stolen, or loaned cards as signature tokens. Further, in order to retain the meaning of a digital signature, creating the signature must be an intentional act. Precautions must ensure that it is not possible to sign a document that the provider intended only to view.

For this reason, it is recommended that smart cards be configured to protect digital signature keys with a password, and that this password be different from the password or passwords used to unlock other features of the card.

Controlling Initial Card Possession

The card issuance process is key to the security of any ID card system. No matter how secure a credential is, it can guarantee nothing if it is given to the wrong person.

Since health care providers typically have some formal association with the facilities in which they work, maintaining control over the issuance process is not difficult. Nevertheless, the issuance process should be defined carefully and reviewed with security, legal, and operational staff to ensure that it meets the needs of the facility without jeopardizing security.

Card Use by Patients

Smart cards can meet a multitude of needs for patients, from providing emergency medical information to acting as a portable key to the patient's medical history, automatically providing personal and insurance information. These different applications require different security measures and best practices.

[19] An example can be found at the CMS website, http://www.cms.hhs.gov/it/roadmap/standards/TRM.pdf or at http://www.hipaadvisory.com/regs.

Accessing Emergency Medical Information

Certain medical information makes the difference between life and death in an emergency situation. The combination of patient smart cards and EMT-carried card readers has the potential to save thousands of lives every year. Access to emergency medical information, however, raises challenging security and technical issues.

In general, patient medical data should be provided only with the patient's permission. In the case of emergencies, however, it is not uncommon for a patient to be unable to grant this permission. In addition, while access to all medical data must be appropriately logged, EMTs may not have access to a central database in which to record such access. Even radio-based communication cannot address this issue completely, since an EMT may be located in an area in which no signal is available.

The recommended solution is to create a storage location on a smart card that can be opened by an authorized EMT smart card reader without requiring permission from the patient. To ensure that patients retain control over what data can be revealed, it is recommended that patients consult with their health care provider and decide what data is placed in this emergency file.

The mechanism used by EMT smart card readers to authenticate themselves to a patient card poses some significant challenges. Addressing these challenges would require a cooperative effort between insurers, and include the Federal government and EMTs nationwide. It would probably be necessary to establish a national certification agency to certify the keys used by EMT readers. When patient cards are issued, they would most likely have to be provided with the information required to validate the certified keys.

Accessing Medical History

Because smart cards cannot store a patient's complete medical history, such information will have to be stored in an online database. Access to a patient's data requires both the patient's permission and provider authentication (for the audit trail). Smart card technology can support both requirements.

Either passwords or biometrics can be used to authorize the smart card to "unlock" the patient's medical history.[20] The use of biometric technology has significant advantages particularly for patients with poor memories or who make infrequent use of health care. Biometrics technology also has some significant disadvantages: patients may not have the body parts that would be measured; patients may find biometrics objectionable (particularly fingerprints, which are often associated with law enforcement); and it is theoretically possible for an unscrupulous individual to manipulate an unconscious patient into unintentionally authorizing the release of information.

It is therefore recommended that individual patients be given the option of using a password or a biometric for authentication. Smart card technology can support the use of either or both. In addition, a backup process must be defined that permits access to the data in the event that the technology cannot be used (e.g., the card or biometric is lost or the password is

[20] For additional information on smart cards and biometrics, see the Smart Card Alliance report "Smart Cards and Biometrics in Privacy-Sensitive Secure Identification Systems," at www.smartcardalliance.org.

forgotten). This process must verify the identity of the patient and authorize the release of the information.

Accessing Personal Information

Health care providers often require certain personal information, such as a patient's name, address, telephone number, or nearest relative. Generally, this information is provided by the patient in written form and then entered into a computer system – a process that is tedious (for both the patient and provider) and error-prone. Smart cards can make this process easier and more accurate, allowing the data to be stored on the card and retrieved as needed, rather than recreated at each opportunity.

Like non-emergency medical information, personal information is private and should not be divulged unintentionally. The recommendations for controlling personal information are therefore the same as for controlling a patient's medical history (with the personal information typically stored on the smart card rather than in a database).

Accessing Insurance Information

Health care providers generally require information about insurance for both emergency and routine (non-emergency) care. Smart cards can store this information and provide it as required.

In emergency situations, it is useful for the provider to be able to access insurance information to start required paperwork, even when the patient may not be able to provide the information or authorize the provider to obtain it. In such situations, smart cards should release insurance information to a provider's smart card reader. In routine care situations, smart cards can provide the information according to the insurer's policy, which may require patient approval.

Because insurance information ages quickly (for example, if an individual changes to an employer with different health insurance plans), it is desirable to verify the information online with the insurer. The card can store both a snapshot of the patient's insurance and information about how to contact the insurer for verification. The snapshot should include a date, so that the provider knows how current the data is.

Insurance information is owned by the insurer (and probably the issuer as well), not by the patient. Therefore, access controls must be implemented according to insurer policy. In the interest of portability, however, it is recommended that insurers either leave this data unprotected or establish a mechanism whereby the information is available to any provider, similar to the mechanism described for protecting and releasing emergency medical information.

Authorizing Decisions Electronically

Like providers, patients must frequently provide signatures authorizing certain decisions (such as decisions about care or payment). The discussion of provider paperless signatures on page 25 applies equally well to patients, with the exception that patients, who use their cards less, may have more difficulty remembering the password required to authorize a digital signature. Although biometric authorization can be used, in the interest of patient comfort, the recommended approach is for the card to protect digital signatures using the same verification required for medical history access

and to require a handwritten signature as well. The handwritten signature can be captured digitally or on paper.

Controlling Initial Card Possession

Secure issuance is the basis of all smart card security. This requirement poses some difficulties for patient cards. Currently, both paper and plastic patient cards are issued based on information provided by the patient on paper forms submitted to a health care insurer or provider. The insurer or provider then issues the card, generally through the mail. This process is very convenient for the patient but is not very secure.

While it is possible to create a secure issuance process, such a process requires that the patient be present in person. The presence of the patient permits the data and patient identification to be thoroughly verified before the card is issued. This approach is probably not feasible in most cases and is certainly inconvenient.

The recommended approach is based on the security principle called "incremental value aggregation." This approach calls for issuing a smart health card in the same way as the current insurance card is issued. However, the card as initially issued contains little or no information of a sensitive nature, cannot provide digital signatures, stores neither passwords nor biometric data, cannot unlock the online medical history, and is marked electronically as being unassociated with the cardholder. The first time the patient visits a provider, the provider requests verification of the patient's identity (e.g., a driver's license) and then allows the patient to set all passwords, link the card to the appropriate online medical history record, and enable the digital signature functionality. This process can be very simple for both the provider and the patient.

In addition, other online verification processes should be implemented so that a patient can fully activate a card from home (using a computer connected to the Internet and an attached smart card reader) or at a kiosk. An adequate level of security can be provided by a combination of authentication factors, such as obscure personal information along with a password mailed to the patient separately from the card. Home- or kiosk-based card access is also an ideal way for a patient to manage emergency medical information (as described in *Accessing Emergency Medical Information* on page 26).

Summary

Smart cards can be an instrumental component of any system that is designed to ensure compliance with HIPAA regulations. Smart cards can also provide significant clinical and administrative benefits that extend beyond HIPAA requirements.

Profiles of Smart Card Health Care Applications

Smart cards have been successfully used in health card applications worldwide. This section describes the efforts of several organizations who have implemented smart health cards.

- University of Pittsburgh Medical Center
- Mississippi Baptist Health Systems
- French Health Card
- German Health Care Card
- Taiwanese Health Care Smart Card Project

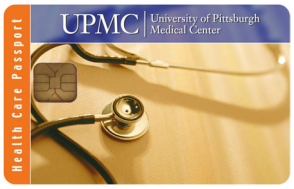
University of Pittsburgh Medical Center[21]

Faced with dramatic growth, the University of Pittsburgh Medical Center (UPMC) found it difficult for their technology infrastructure to keep up with their business requirements. Given their size – 20 hospitals and a group of over 5,000 doctors in over 400 offices – processes such as verifying the eligibility of individuals while maintaining the confidentiality of sensitive patient information became increasingly difficult. UPMC found that it was obvious they were moving toward unmanageable administrative processes, high and increasing operational costs and ineffective intra-health system communications.

An initiative was undertaken to implement a solution that would integrate UPMC's disparate systems and practices. The mandate for this system would be to:

- Solve the challenges of complying with data privacy and confidentiality legislation (i.e., HIPAA) requiring higher security.
- Enable patients to have access to their information and play a part in updating their data.
- Provide a portable solution capable of immediate access and consistent data flow.

UPMC determined that smart cards were the obvious choice as the centerpiece in this new system.



Following a successful two-year pilot project – in which approximately 300 cards were distributed to UPMC Health Plan subscribers, and one physician's office was equipped with readers – the UPMC smart card, called the Healthcare Passport, has now been distributed to 2,000 UPMC patients, 1,000 UPMC physicians and five members of the Chip Ganassi NASCAR racing team. This is the next phase of a five-year, $500 million electronic medical records initiative.

For the patient, the immediate benefits include speeding the check-in process during office visits. The cards enable better care through faster retrieval of important medical information, according to Scott Gilstrap, director for technology solutions at UPMC. "The smart card eliminates a lot

[21] Sources: Scott Gilstrap and Christine Henderson, University of Pittsburgh Medical Center, www.upmc.com; Alegra Technologies, www.alegratechnologies.com.

of paperwork for the patient and makes the visit to the doctor more convenient and less stressful," Mr. Gilstrap said. "It can be a true lifesaver, especially for the elderly who may not remember all of the medications they are taking. This information is stored, updated accurately and easily available on the card."

Patients will no longer need to fill out their personal information each time they visit their doctors since the cards will contain pertinent critical information such as medications, allergies and chronic conditions. By inserting the patient card in a computer in the exam room, the physician can have instant access to accurate and up-to-date information on the patient.

Patients can also check their stored information by using a computer kiosk in the physician's office or they may purchase a card reader to use with a home computer. For the patient, a PIN is required to gain access to their data.

In addition to patient use of smart cards, 1,000 medical staff physicians and affiliated physicians from UPMC will also have cards. Physicians will be able to access information on their patients from home or office using their smart cards. These cards are being called MDID – Medical Digital Identification.

"The key is to give physicians access at home, comply with HIPAA privacy and security rules and make it easy for UPMC physicians to view vital health information and take better care of their patients at our facilities," said Ralph Schwartz, M.D., director of UPMC MedCall. UPMC MedCall is an extensive physician tracking system that includes immediate contact information of more than 14,000 UPMC physicians that is available 24 hours per day, seven days per week, maintains more than 400 on-call schedules, and is considered among the largest electronic physician tracking systems in the United States.

The UPMC smart card uses sophisticated security measures that make it nearly impossible for strangers or unauthorized personnel to retrieve a patient's medical information. "In order to access information, each patient and physician must have a card and a PIN. This is called two-factor authentication. One piece of authentication is useless without the other," Dr. Schwartz said.

The cards also may decrease the likelihood of inaccurate billing. About 90 percent of services denied by insurance companies are due to clerical errors made at the time of registration for a clinical service.

Because of the numerous UPMC facilities and the need for an integrated system, the software and integration applications of the smart card were developed by UPMC's Information Technology Division.

The card contains 64 KB of EEPROM that is devoted to data storage. The data are stored using compression technology with a 10-to-1 compression ratio, allowing 640KB of information to be stored on the card. (640KB is the same capacity as some of the earlier computers.)

Soon, paramedics and emergency rooms equipped with card readers will be able to rapidly access potentially life-saving information about a patient, such as allergies to medications and chronic medical conditions. The initial rollout will include smart card readers at the Presbyterian University Hospital Emergency Department, Sports Medicine in the Kaufmann Building, Sports Medicine in Southside and Dr. Solano's practice in Oakland, Pennsylvania.

"It won't be long before most, if not all, emergency departments and physician offices, even those not affiliated with UPMC, will have smart card readers, which currently cost less than $20. Readers are already being

integrated into most of the newer personal computers. There is every reason to believe that the technology will soon be in medicine," Mr. Gilstrap explained. "This technology not only solves our immediate security concerns for granting access to electronic health records, but also provides a feature-rich alternative to include a host of other applications which provide improved medical care, improved access and convenience of care, and at the same time enhance our business relationships."

The smart card project is just one component of an ambitious information technology initiative at UPMC. The centerpiece of the initiative is the development of an electronic health record to be totally integrated across the entire system, which includes 17 hospitals in both urban and rural settings, hundreds of physician practice offices, and nursing, personal care and long-term care facilities.

The goal of UPMC's information technology initiative is to improve the quality of patient care, to reduce errors and duplication of services and to be a more cost-effective system. Importantly, UPMC believes information technology allows patients greater access to care and a more informed, interactive health care experience.

Mississippi Baptist Health Systems[22]

Starting with two doctors in 1911, Mississippi Baptist Health Systems (MBHS) now comprises two hospitals (Mississippi Baptist Medical Center and Baptist Restorative Care Hospital), 500 doctors on staff, 110,000 emergency room outpatients a year, and a host of health-related services in the community. In an attempt to stay ahead of the legislated requirements of HIPAA, MBHS has begun work on a smart card-based program to replace their current magnetic stripe identification card system. The added bonus of being able to use multiple applications on a single card was also a factor in deciding to use smart cards.

To the 70,000 current card-carrying members of their system, MBHS hopes to reach new levels of patient convenience, safety and privacy with the smart card program. Their goal is to replace all legacy cards within two years of the institution of the new program. In addition to the functionality provided by the new smart card program, MBHS also hopes to gain visibility from its initiative, marking it as a leader in health care technology.

The cards will contain a subset of the patient's medical record and demographic information. When visiting a doctor's office, emergency room or clinic, upon presentation of the patient's card, a form specific to the site visited will print out. The card will maintain a record of clinical history such as blood pressure, pulse, and medications. In the future, the cards will be used to fax medical records from incoming ambulances to the destination emergency rooms.

MBHS is using in-house developers to integrate the new technology into their existing data infrastructure. Using Java Card programming, they have developed their own Internet update and maintenance programs. They have also created their own user interfaces and have designed clinic kiosks for on-site patient use. The initial pilot is scheduled for October 2003 with full production to follow before the end of the year.

[22] Source: Alegra Technologies, www.alegratechnologies.com; Mississippi Baptist Health Systems.

French Health Card[23]

Background

Starting in 1997, France began a complete reform of health care organizations and professionals. The purpose was to develop a program meeting the data exchange expectations and needs of everyone involved in French health care, from insured patients to health care professionals and insurance funds.

France was one of the first countries in the world to introduce large scale deployment of smart cards as part of a health insurance system. The system, known as Sesam Vitale, was the first completely automatic system in which smart cards were used in the health sector. Today, there are approximately 57 million cards in use. That number is expected to rise to 65 million in the near future.

Health care in France is funded partly by the French government and partly by private insurance companies. This situation leads to a complex process for reimbursement for the individuals involved, both patients and professionals. The old paper system was prone to error, fraud, and long delays before final payment was received.

Sesam Vitale

Sesam Vitale is a highly secure dual-card system. The cards (one for patients and one for health care professionals) are the heart of a French health care system that links every individual with health care resources, including public hospitals, private clinics, general practitioners, specialist doctors, nurses, and midwives, all through a secure network. The Sesam Vitale system simplifies the procedure by which health care costs are cleared and also dramatically reduces the risks that refunds to insured patients will be delayed by replacing an annual 1 billion pages of health care information with electronic transactions. The result is that the average reimbursement time has been reduced from up to 6 weeks to 2 or 3 days. In addition, payments are made directly to health professionals by the insurance companies. The system also tracks health care spending and, in the future, will be used to transfer electronic prescriptions to the health care funds responsible for reimbursement.

Sesam Vitale Patient's Card

The Sesam Vitale patient's card is a microcontroller card containing approximately 4 pages of text. The patient's surname, first name, and Numéro d'inscription au Répertoire (NIR)[24] are printed on the front of the card. On the back is the card serial number.

[23] Sources: Atmel Corporation, www.atmel.com; http://www.smartcard.co.uk/resources/articles; http://www.sesam-vitale.fr.

[24] The NIR is the French equivalent to the U.S. social security number; however, no credit bureau is allowed to gather financial information using the NIR. This eliminates the use of the number for identity theft.

The data stored in the chip are separated into two zones and include the NIR, health insurance system code, branch, entitlement start date, proof of entitlement, presence of permanent entitlement, surname, first name, date of birth, status of beneficiary, information specific to the health insurance system, and entitlement end date. The card replaces the standard "soft copy" individual health insurance card.

The first, family version of the card (Vitale1) contains administrative data that is available to health professionals (such as physicians, pharmacists, dentists, physiotherapists, and nurses). The data is read immediately and stored as a secure electronic health care cost claim sheet (e-sheet) during the patient visit. (The data cannot be read without the presence of a health care professional's card, or CPS, described below.) Depending on the software application and the smart card reader, this e-sheet can be stored either in programmable secure reader memory or on the health professional computer's hard disk. The sheets are bound daily into secure electronic batches and transmitted through the secure national health intranet, the RSS (Réseau Santé Social), to the health insurance front-end servers. There the sheets are automatically processed by a back-office system for further cost clearing.

Sesam Vitale Health Care Professional's Card

The Sesam Vitale health care professional's card, called the Carte de Professionnel de Santé (CPS), is also a highly secure smart card that is easily recognized by its color. The MCU embedded in the card includes a crypto-processor that manages public keys and generates digital signatures.

The card identifies the health care professional and provides authentication, digital signatures, and data encryption. Pharmacists and medical staff also receive a card. More than 425,000 cards have already been issued to health care professionals, with more than 90,000 to physicians.

German Health Care Card[25]

Health insurance is required in Germany, and the majority of the population is served by public health insurance. Currently, Germans carry a health care card that can be characterized as an insurance card. Its primary function is administrative.

Current Health Card Program

The current German health card program was rolled out in 1993 and is fully implemented. A total of 80 million people now carry the card. The card contains a 256 byte protected memory chip (not an MCU) and stores the following data:

- Identity of the insurance.
- Insured person's name, address, and date of birth.

[25] Source: Infineon Technologies, www.infineon.com.

- Status of the insurance.
- Expiration date for the insurance.

This data supports for the following administrative benefits:

- Patient identification.
- Elimination of duplicate records.
- Reduced paperwork and cost associated with mailing health insurance forms.
- Streamlined admission process.
- Reduced transaction costs.

A 1997 study by the German Ministry of Health showed that the cost of the cards was fully amortized in the 3 years after introduction.

When data on the card become obsolete, insurers reissue the card (even though overwriting the obsolete data is possible). Between 15 and 20 million cards are issued annually.

Next Generation Health Card Program

Germany is now planning for the next generation of health care cards. The new program is expected to include cards for patients and cards for health care professionals. These more advanced cards will be based on 16 KB or 32 KB microprocessors. The cards are expected to provide multiple additional benefits, such as enabling insurers to collect co-payments that are currently uncollected and eliminating paperwork associated with the current prescription drug program.

Trials of the new program are expected in 2004-2005, with January 2006 the target date for rollout. The expected total cost to upgrade the system infra-structure and issue new cards is approximately $500 million. Although this figure sounds high, a study commissioned by the Federal Association of Pharmacists and one of the country's health insurance funds and undertaken by Hamburg-based health consulting firm Debold & Lux predicts that the new health card system could pay for itself within 12 months.

Many health care professionals in Germany would also like to see an electronic prescription drug application. The Minister of Health is investigating potential pilots for such an application.

The Taiwan Health Care Smart Card Project[26]

The Taiwan health care smart card project is one of the largest health care smart card solutions in the world and the first of its kind in Taiwan, Republic of China. The total bid price for the project was US$108 million, and contractors were requested to finish within 25 months of the start date, April 12, 2001. The smart card project infrastructure is integrated into the original paper-based health care system.

[26] Source: MartSoft Corporation, www.martsoft.com. Special thanks to Mr. K.P. Chang and Ms. Tiffany Lee for providing interviews and access to reports about the Taiwan health care smart card.

Project Background[27,28,29]

The total population of Taiwan is now 22.5 million, and 96% of Taiwan citizens joined the National Health Insurance (NHI) program that was established 8 years ago. A total of 16,558 hospitals and clinics (90% of the total) registered in the NHI program, creating a service network for insured applicants nationwide. Taiwan had a strong IT foundation: the original paper-based health care system included 92% of contracted medical institutions with a computerization rate of at least 70% and public satisfaction levels of 71%.

The NHI program recognized revenue from insurance premiums of US$8.3 billion in 2001. Total health expenditure is 5.5% of Taiwan's GDP.

Before the smart card was introduced, paper cards were used by the Bureau of National Health Insurance (BNHI) to audit patient information, then reimburse service providers monthly. The card is renewed after the patient uses medical services up to six times. Even though reporting and information handling is well run and maintained, the system has certain problems, such as identity fraud, excess false insurance premium claims from health care institutions, complex program vouchers, waste of resources due to high frequency of card replacement, and high losses due to discontinuity of insured applicants. To solve these problems, in April 2001 the Bureau of National Health Insurance (BNHI) issued 22 million smart health care cards using Java Card technology to Taiwanese citizens.

Project Implementation

The main contractor, the Smart Card Division of the Information System & Service Sector of TECO Electric & Machinery Co., Ltd. (TECO),[27] integrated the original back-end database for the paper card system with the interface for the new smart card system. In the first year, they created specifications that met the requirements for hospitals and clinics, computer back-end needs, security rules, and networks. They also completed the system development required by the specifications. In the second year, TECO manufactured the cards, developed the required applets to be loaded on the cards, audited the information for all 22 million people, took photographs, issued cards to everyone, and installed card readers in 16,000 participating hospitals. They also tested and verified all processes. Currently about 70% of the hospitals are online. It is believed that the online rate will be almost complete by the end of 2003.

This project required multiple stages. The tasks for the main contractor included the following:

- Design and facilitate the execution of security policies.
- Allocate resources to design, manufacture, and distribute approximately 22.3 million smart cards and 300,000 reader security access module (SAM) cards.

---

[27] Taiwan Bureau of National Health Insurance web site, www.nhi.gov.tw (in Chinese), news articles; www.nhi.gov.tw/01intro/intro_5.htm (in Chinese); www.win2000.com.tw/teeth/iccard.php?menu=5 (in Chinese).

[28] *National Health Insurance: An Overview and Perspectives*, Bureau of National Health Insurance, Taiwan, 2002.

[29] Interview with Mr. K. P. Chang from TECO Electric and Machinery Co., Ltd., by Matt Wylie, TECO.

- Install 20,000 free reader sets (one for each health institution in the pilot trial).
- Establish and manage a 150-seat call center for card use support.
- Develop a comprehensive computing network between BNHI headquarters and its branches and develop a medical VPN.
- Integrate a platform for information transmission between BNHI, hospitals with different health information systems, and medical institutions with different IT infrastructures.
- Manage 800 training courses for end users and hospitals nationwide.

Project Results

TECO and the other participating entities integrated the entire IT infrastructure of Taiwan's health industry and then integrated this new infrastructure with a secure smart card solution.

The NHI health care smart card (illustrated below) can be used for 5 to 7 years, making annual replacement unnecessary. The front side of the card includes the card's serial number and the cardholder's photo, name, ID number, and date of birth. People are not required to present an additional ID when they use the card for NHI health care services.

The smart card is a microcontroller-based card and has 32 KB of memory, of which 22 KB will be used for four kinds of information:

- Personal information, including the card serial number, date of issue and cardholder's name, gender, date of birth, ID number, and picture.
- NHI-related information, including cardholder status, remarks for catastrophic diseases, number of visits and admissions, use of NHI health prevention programs, cardholder's premium records, accumulated medical expenditure records and amount of cost-sharing.
- Medical service information, including drug allergy history and long-term prescriptions of ambulatory care and certain medical treatments. This information is planned to be gradually added depending on how health care providers adapt to the system.
- Public health administration information (such as the cardholder's personal immunization chart and instructions for organ donation).

The Taiwanese government has reserved the other 10 KB of memory for future use.

Moving to the smart card system has resulted in the following changes:

- Hospitals and clinics upload electronic records daily to BNHI.
- After every six patient visits, card information is uploaded online for data analysis, audit, and authentication.
- The reimbursement process is faster.

Privacy and Security[30]

BNHI has strong privacy and security requirements for the Taiwan health care smart card, including a defined privacy policy, multiple smart card security mechanisms to prevent counterfeiting and protect cardholder information, mechanisms to protect the security of information during transmission, practices to prevent computer viruses and a crisis management and response plan. The overall system architecture was designed to implement these policies, protecting the cardholder's private information while allowing access by authorized health care professionals. Key smart card security and privacy mechanisms are:

- High-grade card printing, comparable to payment cards.
- Encryption of information stored on the card.
- BNHI-issued Security Access Module (SAM) card for each smart card reader, with a strict authorization and mutual authentication process to access on-card data.
- Cardholder PINs to protect on-card personal information.
- Plans for a health professional card that would be used to authorize health care provider access to medical information on the card.

Lessons Learned[31]

To be successful, similar smart card projects must ensure physical, platform and application interoperability. The following items are important for successful project implementation:

- A comprehensive system security plan to guard the cardholder privacy.
- Certification of security control at each step.
- A comprehensive plan for managing the first issuance of the card, which must involve as few errors as possible to reduce cost.
- A comprehensive plan for the entire information system structure.
- An assessment of the efficiency of system operations.
- A marketing project plan.
- Integration testing and acceptance procedures.
- Card application development to ensure that the necessary card applications are available when needed.

The infrastructure development required to support the Taiwan health care smart card project is well underway. Starting July 1, 2003, both health care smart cards and paper cards are in use simultaneously in Taiwan. As of September 6, 2003, smart cards have been issued to 95% of the population of Taiwan and 70% of the hospitals and clinics are on line and in operation for smart card usage. It is estimated that by January 2004, health care smart cards will be fully implemented and paper cards will be phased out.[32] In the

[30] Taiwan Bureau of National Health Insurance National Heath Insurance IC Card web site, http://www.enhi.com.tw/ (in Chinese). For an English translation, please see http://www.martsoft.com/reference/healthcare/tw_nhi_2003Sep.doc.

[31] "Eight key areas in successful smart card deployment," by TECO Smart Card Business Center, March 2003 (in Chinese).

[32] Taiwan Bureau of National Health Insurance National Health Insurance IC Card web site, http://www.enhi.com.tw/news_detail.asp?file_id=4201.

current (initial) stage, only name, date of birth, and national ID number are stored in the card.[33]

[33]Taiwan Bureau of National Health Insurance National Health Insurance IC Card web site, http://www.enhi.com.tw/news_detail.asp?file_id=4396.

Implementation Success Factors

Smart cards represent an approach to compliance with the HIPAA privacy and security requirements that can also enhance current business processes. The ability to use secure data retained on a smart card to verify the identity of a subscriber or patient is the initial link in the chain of trust between patient, provider, and health plan mandated by HIPAA.

Successful implementation of a privacy-sensitive and secure smart card system for a HIPAA-compliant health care application is a complex, large-scale information technology project that may extend across multiple organizations. The fundamental challenge of any such project is to visualize correctly the system's overall operation and the benefits to all stakeholders (especially the end users) and then express that vision as a series of concrete milestones.

Following proven "best practices" can mitigate any risks associated with such a project and maximize the benefits of adopting smart cards. Such a methodology incorporates an end-to-end lifecycle approach to implementation, addressing all processes from requirements analysis to design, delivery, and long-term maintenance and support.

Developing a Project Delivery Methodology

The probability that a smart card implementation project will be completed on time and on budget is improved when the project is planned and guided according to a well-designed project delivery methodology that is executed by competent project managers and technical resources. Such a methodology is typically a series of step-by-step guidelines for developing, upgrading, improving, or replacing the current business information systems. Sound methodologies identify the tasks, techniques, and deliverables required for successful completion of the project.

In addition, for a project to be successful, all of the stakeholders involved must clearly understand why the project is being undertaken, what work product is expected from the project, who is responsible for the different activities, how project communications will be handled, when deliverables must be completed and, most importantly, what rules govern the entire process. The methodology is a key factor for providing this information.

A generic project delivery methodology includes the following phases:

Phase	Phase Description
Requirements Definition	Identifies and documents the business, technical, and end-user functional requirements for the project.
Conceptual Design	Analyzes business needs from application, network, and operating perspectives. Develops logical object and event models, distribution models, and operation models for different system alternatives.
Detail Design	Uses the models developed in the conceptual design phase to develop detailed specifications. Develops transition plans, a conversion approach, and a test strategy.
Development	Codes and tests the components and programs specified in the detail design.
Integration and Test	Installs new hardware and application components, trains users, and tests new components in an integrated environment. Tests transition plans.
Installation	Performs all conversions and installs the new application in a production environment.

Selecting Project Personnel

Selecting appropriately skilled personnel to implement a project is a key component of success. The project manager (or managers) should have a thorough understanding of the principles and processes of smart card system implementation and be skilled in managing the scope, schedule, and resources for the project. In addition, every project manager, coordinator and technical leader should have expertise in the HIPAA Privacy and Security Rules and in National Institute of Standards and Technology (NIST) standards and other Security Rule reference standards.

Establishing Objectives

One key initial activity is to establish the health care organization's objectives. For example, the objectives of a smart card system implementation could include the following:

- Promote health care as opposed to hospital care.
- Ensure the confidentiality of highly sensitive medical data.
- Enable a higher level of service to system constituents by improving processing time and data accuracy.
- Ensure secure data transmission and storage.

Specific project objectives might therefore include the following:

- Provide a means for constituents to transport core health care registration data.
- Provide strong authentication and digital signature capability.
- Reduce data entry errors on records.
- Encourage the use of electronic business methods.
- Implement one smart health card across the entire enterprise.
- Be honored by all facilities and all employees.
- Provide network-centric, not card-centric, services.
- Securely store clinical and administrative data on one card.
- Be able to change information more easily.
- Provide support for future applications, such as card interaction with kiosks).

Defining Requirements

The functional requirements for a new system must maximize the benefits of the system while minimizing costs. It is critical that every requirement support a stated project objective. In addition, each requirement must be described as unambiguously as possible. This clarification process helps contain overall project cost. The cost to recover from false assumptions in the requirements definition phase increases almost exponentially during later phases.

Figure 6: Relative Cost to Fix Errors Created by False Assumptions in the Requirements Phase [34]

Phase in Which Error Is Found	Cost Ratio to Recover
Requirements	1
Design	3-6
Development	10
Integration	15-40
Acceptance Testing	30-70
Operation	40-1000+

Determining Whether to Build or Buy

One initial design decision is critical: whether to build the required system components or acquire off-the-shelf components. The design team must research the market for viable commercial off-the-shelf systems while also investigating the feasibility of designing a custom application. It is also possible to blend the two approaches.

One issue in the build or buy decision is cost. For example, it is typically more cost-effective to buy software that addresses a business problem when the problem is common to many businesses. The software vendor amortizes the cost of development over a large number of customers. The costs of in-house development can only be amortized across one company.

Another issue in the decision is how to meet HIPAA requirements. HIPAA requires use of ANSI standards. The requirement to use such standards can affect application design as well as the cost of building an application.

A third issue is whether either option has legal ramifications.

Designing the Smart Card

Deciding on a card design forces decisions about the silicon provider, chip type and memory size, chip security, card operating system, forward and backward compatibility, future enhancements, durability, and reliability.

The design also includes identification of the data that will be included on a card. These data must be selected carefully. One question is the amount of clinical data to record on the card. Another is the volatility of the data – the more often the data change, the more often an updated card must be issued to the cardholder or the more often the cardholder must present a card for updating. Yet another is whether to include static data on the face of the card. The more static the data, the less often the card must be reissued.

To be effective, any smart card must support the most common HIPAA-mandated health care transactions, such as a 270 eligibility inquiry, an 837 health care claim, the NCPDP pharmacy claim, and a 278 authorization/ referral request. Patient and subscriber data encoded on the card should

[34] *Exploring Requirements: Quality Before Design*, Donald Gause, New York: Dorset House Publishing, 1989.

include the data elements common to these HIPAA transactions. Including such data eliminates the potential for errors associated with manual entry of patient and subscriber data.

Selecting the Smart Card Reader

The smart card reader is the single point of access for a smart card application. Smart card-based logical access (e.g., controlling access to a network or online resources) typically uses contact cards and readers where the card is inserted into a reader connected to a computer. Physical access control typically uses contactless technology to meet requirements for faster throughput. If a card user needs both physical and logical access, multiple interface smart cards (contact and contactless) can be used with either reader type.

The reader also provides critical functionality for overall system security. For example, an integrated PIN pad or biometric reader may be required to provide a third factor for authentication. Other considerations include how to implement reader security and communication between the reader and other system components.

Data Center and Infrastructure Decisions

The data center is the central component of a smart card system. Included in the data center is network connectivity that allows the smart card readers and host computer to communicate. The design of the data center is therefore critical to system security, overall system functionality, future enhancements, data mining and reporting, and help desk and customer service. If the system is a completely new smart card implementation, another important consideration is whether to support backward compatibility with legacy systems and what impact the change will have on such systems.

Enrolling Cardholders

Project requirements must include not only card and system design but also describe how to accomplish enrollment. Enrollment stations capture card demographic and biometric data from card users. The duration of the enrollment phase of the project depends on the average time it takes to enroll a user, the number of enrollment stations deployed, the hours per day the stations are operational, and the total number of enrollees.

Producing and Issuing Cards

Health care organizations need to determine the appropriate strategy for issuing and delivering cards that meets their requirements. There are three basic approaches to producing cards and issuing them to cardholders: central issuance, over-the-counter (OTC) issuance, or a hybrid (combination of both) approach.

Issuing cards from a central facility can be handled by using an in-house high-volume production system to create the cards or by contracting with a third party vendor for the actual production and distribution of the cards. Some key questions to ask are: Does the provider have a reference site similar to the new system to be implemented? Does a card management system track all cards, identifying those that are printed, issued, rejected, destroyed, or otherwise not completed? Can the provider ensure that the data are correctly printed on both sides of the correct card? How will the cards be distributed if produced centrally?

Over-the-counter (OTC) issuance solutions are typically selected when speed of delivery or decentralized system architecture are important. OTC solutions raise questions about security and maintenance support. When cards are issued from distributed locations, card materials must be present at each location and personnel must operate the equipment with little or no supervision. This situation presents an opportunity for fraud. In addition, because locations are distributed, maintenance support may not be readily available. An organization selecting the OTC solution can sometimes reduce risk by selecting third-party providers with a local presence.

The hybrid solution is an option for organizations requiring a combination of both approaches (e.g., when an organization needs periodic issuance of a large number of cards from a central facility and incremental OTC issuance of cards for new employees). The main drawback of the hybrid approach is that all cards may not be identical. An organization can reduce this risk by specifying card design and layout carefully and completely in the requirements document, including in the specification such details as the card look-and-feel and desired image resolution and font sizes.

It is important to note that not all card materials or card production techniques are equally appropriate for both central and OTC solutions. Before deciding how cards will be produced, it is important to determine whether the candidate card materials and production systems have been used successfully to handle similar production volumes before.

Managing Card Lifecycles

Card lifecycles begin with the recognition that a card must be issued. The lifecycle includes events such as card renewal and update, as well as replacement of lost or stolen cards.

The lifecycle of a smart card can be as long as 10 years. It is important to consider both the economics and timing of card updates. For example, existing cards may be able to be updated electronically (data and/or applications) or new cards can be issued – resulting in different implementation and on-going costs. Cards may need to be updated at various intervals, sometimes as often as annually, and the update process must be rapid and secure. In addition, cards must also be withdrawn from service when cardholders are no longer eligible for the health care supported by the card provider (for example, when employees change jobs).

One important consideration in lifecycle management is whether to issue cards as active or inactive. Many entities within the health care industry that use cards distribute the cards as inactive cards to ensure that cards are distributed to the real owner and to prevent fraud from cards stolen during the distribution process. The subscriber is required to activate the card upon receipt.

If inactive cards are issued, the telephone and Internet activation process in place for credit cards could be used to activate the card. When determining whether to distribute a card as an active card or an inactive card, it is important to consider what information and services can be accessed by the cardholder.

Project Management Discipline

As with all large-scale information system projects, organizations must take a disciplined approach to project management throughout the entire process. This includes having a quality management process, managing and controlling risk, developing and using test and acceptance metrics,

determining whether to outsource any project functions, keeping the project on budget, developing user training and documentation, and providing for on-going help desk and system maintenance support. Project personnel must factor into the process how to comply with any HIPAA rules that need to be incorporated.

Summary

There are six keys to implementing a smart card system successfully:

- **Planning**. Health care enterprises that have successfully implemented smart card systems point to thorough planning as one key to success. For large-scale health smart card deployments, implementation may require agreement on new business policies and practices that extend across multiple organizations. It is necessary to plan the management of information before thinking about the technologies to be used. Most important is to identify how the project contributes to the organization's goals.
- **Choose carefully**. When evaluating suppliers, identify those with proven experience and deep technical resources. When considering a systems integrator, ensure that the integrator's subcontracted partners are highly experienced, "best-of-breed" technology suppliers. Consider whether the integrator has a large enough local presence to implement and support the smart card system at all required locations. Also evaluate whether your staff is compatible with the integrator's staff.
- **Start at the top.** It is critical that the highest level of executives within an organization understand the project and commit themselves to its success.
- **Talk early and often.** Ensure that project members and other staff members work in tandem and share knowledge.
- **Beware of scope creep**. Functional requirements tend to grow during the implementation process. At the outset, collaborate with suppliers to identify who is responsible for what tasks and establish measurable parameters to keep the project on time and on budget.
- **Evaluate progress frequently**. Set milestones for deliverables to measure the project's progress, evaluate suppliers' work, and ensure that all primary goals are being met.

Conclusion

Health care organizations are implementing new policies, processes, and technologies to comply with HIPAA requirements for security and privacy of health information. HIPAA requires all health care organizations that create or maintain electronically protected health information to secure that information from any intentional or unintentional use or disclosure that violates the HIPAA Privacy Rule. It is critical that health care organizations put in place mechanisms that balance the need to maintain the privacy and security of patient information with the need to efficiently access that information and ensure quality care.

Many technologies can be used to provide secure, authenticated access to health care information, including technologies that secure both physical and logical access. Systems that use smart cards as the identity token and secure data carrier have unique benefits.

- Smart cards can provide easier information access management, ensuring that users are following established security policies.
- Smart cards are a familiar form factor that can be used for both physical access to facilities and logical access to information on personal computers and networks.
- Smart cards can help enforce access control to health information, providing support for both user authentication and encryption of data on the card and during transmission and storage.
- Smart cards can store health information on the card, performing as secure portable data carriers that are under the control of the patient and the health care professional.
- Smart cards, with on-card intelligence and processing capabilities, are uniquely capable of enabling compliance with strong privacy guidelines and of enforcing the privacy and security policies set by the health care organization.
- Smart cards provide a feature-rich platform for health care organizations to implement new applications that improve access to and convenience of medical care.

Smart cards are being used worldwide to provide improved security and privacy and to add new features in financial, enterprise and government identification, and health care applications. The Smart Card Alliance urges health care organizations implementing systems that meet HIPAA requirements to familiarize themselves with how smart cards can both deliver enhanced security and privacy and support new applications that deliver clinical and administrative benefits.

For more information about smart cards and the role that they play in health care, secure identification and other applications, please visit the Smart Card Alliance web site at www.smartcardalliance.org or contact the Smart Card Alliance directly at 1-800-556-6828.

References and Resources

Centers for Medicare and Medicaid Services web site, http://www.cms.hhs.gov/hipaa/.

Dataquest: Worldwide Chip Card and Semiconductor Vendor Market Share, 2002 *Focus Report*, April 24, 2003.

"Eight key areas in successful smart card deployment," by TECO Smart Card Business Center, March 2003 (in Chinese).

Exploring Requirements: Quality Before Design, Donald Gause, New York: Dorset House Publishing, 1989.

"The Future of Card Technology in Health Care," by Beckie Kelly, *Health Data Management*, May 2002.

HIPAAdvisory web site, http://www.hipaadvisory.org.

"HIPAA's Long and Winding Road," by Joseph Goedert, *Health Data Management*, March 7, 2003.

"Hospital Strengthens Network Security with Smart Cards and Biometrics," *Card Technology*, January 31, 2003.

"Is the Future in the Cards?" by Deborah R. Dakins, *Health Data Management*, July 2001.

Mobile Healthcare Alliance, http://www.mohca.org.

National Health Insurance: An Overview and Perspectives, Bureau of National Health Insurance, Taiwan, 2002.

Planning for PKI, by Russ Hously and Tim Polk, John Wiley & Sons, 2001.

"Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology," Smart Card Alliance white paper, February 2003.

Sesam-Vitale web site, http://www.sesam-vitale.fr/.

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

"Smart Cards and Biometrics in Privacy-Sensitive Secure Identification Systems," Smart Card Alliance report, May 2002.

"Smart Cards as Enabling Technology for Future-Proof Healthcare: A Requirements Survey," *Open Smart Card Infrastructure for Europe v2*, Volume 1, Part 4, www.eeurope-smartcards.org.

Taiwan Bureau of National Health Insurance web site, www.nhi.gov.tw (in Chinese).

Taiwan Bureau of National Health Insurance National Health Insurance IC Card web site, http://www.enhi.com.tw/.

U.S. Department of Health and Human Services, Office for Civil Rights, *Standards for Privacy of Individually Identifiable Health Information*, [45 CFR Parts 160 and 164].

U.S. Department of Health and Human Services, Office for Civil Rights, *Standards for Privacy of Individually Identifiable Health Information,* [45 CFR Part 142 – Security and Electronic Signature Standards].

WLAN Smart Card Consortium, http://www.wlansmartcard.org.

Publication Acknowledgements

This report was developed by the Smart Card Alliance to discuss how smart cards can help health care organizations meet HIPAA's privacy and security requirements. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Secure Personal ID Task Force members for their contributions. Participants from 19 organizations were involved in the development of this report including: Alegra Technologies, Atmel Corporation, Datakey, Gemplus, IBM, Infineon Technologies, Lockheed Martin Management and Data Systems, MartSoft Corporation, Mississippi Baptist Health Systems, Northrop Grumman Information Technology, Privamed, Inc., Raak Technologies, Smart Commerce Inc., Security Sciences International, Taiwan Bureau of National Health Insurance, TecSec, University of Pittsburgh Medical Center, Unisys, Wave Systems.

Special thanks go to the individuals who wrote, reviewed and edited this report.

David Asay, IBM
Linda Brown, Infineon Technologies
John Butterworth, Security Sciences International
Jim Canfield, Alegra Technologies
Yuh-Ning Chen, Ph.D., MartSoft Corporation
Jay Cornish, Unisys
Ian Duthie, Atmel Corporation
Mansour Karimzadeh, Smart Commerce, Inc.
Colleen Kulhanek, Datakey
Gilles Lisimaque, Gemplus
Louis Liu, Taiwan Bureau of National Health Insurance
Mark McGovern, Lockheed Martin Management and Data Systems
Cathy Medich, Consultant and Task Force Chair
Fred Namdar, Privamed, Inc.
Jay Wack, TecSec
Bob Wilberger, Northrop Grumman Information Technology
Shawn Willden, IBM
Erik Wilson, Raak Technologies

Copyright Notice

Trademark Notice