Swipe and Say 'Aaah': Managing Patient Health Data on Secure Smart Cards

by Henry Zach

Sharing data electronically rather than verbally or on paper benefits healthcare by reducing medical errors, improving the quality of routine and emergency care, and lowering administrative costs. Capturing and transmitting information digitally also ensures patients and providers are able to share health information in a secure format.

A smart card with an embedded computer chip and microprocessor is a patient-focused health data storage system. The smart card system provides portable and secure health information to be transmitted from the patient to the provider, provider to provider, and provider back to the patient.

Digital information on a smart card can be printed to bridge existing paper-based information channels and to allow patients to review their health information. The information on the card is not an electronic medical record, but a digital data storage tool designed to assist patients in providing accurate medical information to providers during routine office visits, admissions to hospitals, or in emergency situations when patients may not be able to speak for themselves.

This article describes one model of how smart cards are used.

Data in Hand

Cards are typically provided to consumers through employers, healthcare networks, and insurance companies. Demographic and personal information saved on the card consists of name, address, marital status, language, age, sex, height, weight, eye color, primary physician, employer, and insurance. Basic medical information includes allergies, daily medications, chronic conditions, and immunizations. Emergency medical and contact information is also included.

As in paper-based systems, patients provide the initial data using a secure online application process or a printed optical character recognition (OCR) application. Digital or OCR data is transferred to the smart card's chip. The loaded card is given to the patient with a printout for patient verification. Later updates to the card may be made at the time of service.

The smart card supports the national health information infrastructure as reported by the National Committee on Vital Health Statistics to the US Department of Health and Human Services. The cards help providers meet two of the three health dimensions—the personal health information and healthcare provider dimensions. With smart cards, consumers have their personal healthcare information at their fingertips, allowing them to control its use and helping them manage their own wellness and healthcare decision making. By providing access to more complete and accurate patient data on the spot and around the clock, smart cards help providers promote quality patient care.

The smart card's data integrity and accuracy includes initial patient-provided data and healthcare provider information written to the micro-processor chip that is embedded in the card. Current distribution of responsibilities to help ensure information integrity is the same as with paper-based systems. Security and accuracy liabilities remain the same.

Updates at the Point of Care

Requirements developed for this system call for an electronic device that stores patient information in a vehicle that is secure, easily updatable, and readily available to medical providers. It is important that the device be easy to maintain and update. This may be done through the physician's office either at check-in or check-out. The end result is that the patient does not need to complete a new medical form for each visit to a new healthcare provider. The physician, nurse, physician assistant, or an office staff member updates the medical records in the office at the time of the patient visit.

Providers can implement the smart card system at a stand-alone workstation or in a local area network using a server and distributed workstations. The workstations can be located wherever they are convenient for the provider—in emergency departments, admitting and reception areas, administrative locations, and in patient and exam rooms. The necessary software is available at no charge to licensed healthcare providers and requires minimum training. Each workstation operating the software requires a smart card reader to read information from and write information to the patient's card. Readers are commericially available at a nominal cost.

Limiting Access

In this model the log-on security process has three user levels: administrative, system, and card user. Card user access allows access to only the patient record information stored on the smart card in the card reader at that time. This limited access works well in an emergency room to protect the information of other patients in the database. System user access allows access to all records in the system's database, as well as the record on the card in the card reader. This access level is used in more secure locations such as a caregiver's office. Administrative user access provides the capability to manage all levels of the user and log files.

Log-on security and access to patient records is administered and controlled at the system administrator level using a control screen in the software. Log-ons are established using a combination of characters for the user ID and password and a designation of user level access.

The software tracks activity on the card and in the system. The system log records log-on name, workstation name, date and time, and the action taken (log in or log out) for each user access event. The card access log tracks the user's log-on name, workstation name, date, and time in addition to the patient's record ID, patient's full name, and the action taken with each record that has been accessed. The administrator can review both logs on screen or can print a report of the respective log for auditing user and system activities. To control unauthorized viewing of patient information on a workstation screen, the administrator can also control system screen timeout intervals in areas with surrounding staff traffic or when a user has left a workstation unattended.

Security Measures

The smart card chip contains a microprocessor and memory chip that give the card the capability to control access while providing secure information storage and information processing. In this model, the security functions embedded in the software encrypt and manage the flow of patient information to and from the microprocessor on the chip to protect the information from unauthorized disclosure. When the software writes patient information to the card, the information is first converted from a readable form to a modified secure form of encryption using public key cryptography. Then the data is highly compressed and finally written to the card. Unique keys, called triple data encryption standard keys, are used in the encryption process to encrypt and decrypt the data multiple times, providing security and maintaining the integrity of the patient medical information.

When patient information is read from the card, the compression and encryption process is reversed and the readable information is restored to its original form on the computer workstation. Additional card security is provided by a unique serial number that is dedicated to the smart card and locked to the patient's name or other unique patient identifiers during card initialization. This makes it improbable that a record will be overwritten or comingled with another patient's data during reading or writing to the card.

Other technologies under review include a public key infrastructure that verifies and authenticates the validity of each party involved in an online transaction and biometrics to authenticate an individual by validating one of the person's physiological features, such as a fingerprint, iris, face, or voice.

Smart cards are secure, portable, and upgradable. As technology and trends move toward an electronic health record, smart cards are a possible solution for protecting health information while increasing its portability.

Henry Zach *(henry@healthdatacard.com) is president of Health Data Card, LLC.*

Article citation:
Zach, Henry. "Swipe and Say 'Aaah': Managing Patient Health Data on Secure Smart Cards." *Journal of AHIMA* 75, no.6 (June 2004): 48-49,56.