

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 microprocessor 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.

by Jill Burrington-Brown, MS, RHIA

Q: Why shouldn't we document incidents or incident reports in the patient's health record? Isn't it a part of the documentation of the patient's care? Don't incident reports become evidence if there is legal action?

A: First, we should define "incident" and the purpose of an incident report. An incident is something that happens that is not consistent with the standard of care, not a natural consequence of the patient's disease, or an out-of-the-ordinary event. The purpose of the incident report is to identify potential problems or risks as well as actual problems that need intervention. A healthcare organization should use the incident reporting system in a quality management program to look for emerging trends and system inadequacies and to provide feedback and education.

A patient's health record should never document or mention an incident report. According to the AHIMA practice brief "Maintaining a Legally Sound Health Record," "When an incident occurs, document the facts of the occurrence in the progress notes. Do not chart that an incident report has been completed or refer to the report in charting."¹

An incident report should not be a method of documenting the patient's care but of documenting the incident, its investigation, and follow-up. The patient's care must be documented completely in the medical record. In this manner, when an incident report is investigated by the appropriate quality review committee, it becomes a part of the peer review process. When the incident report is mentioned in the medical record, it then becomes part of the patient care documentation and may be discoverable in states where protection is in place to prevent discovery.

In many states, incident reports have historically been protected from discovery as part of this peer review process. However, in recent years the definition of peer review has narrowed.² The Pennsylvania courts found in *Pennsylvania Protection and Advocacy, Inc. versus Houstoun* (228 F.3d 423 [3rd Cir.2000]) that "the requested peer review documents were records" as defined by the Protection and Advocacy for Mentally Ill Individuals Act and were not protected.³

Additionally, in *AMISUB, Inc. versus Buckley* (618 N.W.2d 684 [Neb.2000]), an incident report created for quality assurance purposes was not reviewed by the hospital's quality committee and did have some patient assessment information that the medical record did not have. Thus, "The state Supreme Court declined to extend the peer review privileges to...the incident reports...." It noted that the documents were not prepared upon the request of a hospital-wide staff committee or utilization review committee. The court found the reports were "merely factual accounts or fact compilations relating to the care of a specific patient [and therefore] are not privileged."⁴

However, in California the courts found that incident reports labeled as confidential documents intended for potential litigation were protected as part of attorney-client privilege and were therefore protected.⁵

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 commercially 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

continued on page 56

continued on page 51

► In Confidence *continued from page 49*



www.cmtcorporation.com

There are Many Reasons to Outsource Clinical Documentation (Not all of them obvious)

Reason #1: *Patient care is your core business, documentation is not.*

Reason #2: *The million-dollar technology you buy today will need upgrades tomorrow.*

Reason #3: *Quantifiable cost saving in a short period of time meets your financial goals.*

Reason #4: *Customizing technology applications is straining your bottom line.*

Reason #5: *Integrating pre-existing legacy systems is straining your bottom line.*

Reason #6: *See below.*

CMT Corporation is the provider of choice for clinical documentation outsourcing services since 1988. CMT does not sell pre-packaged medical transcription services and technology. Instead, we partner with each organization to come up with cost-effective solutions that streamline documentation processes, improve turnaround times, and truly meet the healthcare provider's specific needs. CMT's customer-centric approach, has consistently delivered benefits for more than 15 years, including:

► **Technology-based solutions.** As a CMT customer, healthcare providers have myriad choices -- digital handheld dictation, telephone dictation, *LocusMD*™ ASP, CPOE software, integration with existing HIS/RIS, ADT feed, stringent security and encryption, et al.

► **Accommodation of multiple user preferences.** CMT is known for delivering customer-centric solutions with an emphasis on using technology to streamline processes rather than forcing radical change in behavior.

► **Cost savings.** The advantages of CMT's one-on-one approach are also seen in the bottom-line. You pay only for what you need, instead of paying for bells and whistles you won't use.

Inquiries:

1-800-656-6848

www.cmtcorporation.com

Security features prevent unauthorized disclosure of patient data, and unique identifiers protect against overwriting or comingling records.

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 time-out 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.



Read more about technology and the EHR in the FORE Library: HIM Body of Knowledge at www.ahima.org.