New Possibilities for Patient Information Storage in a Technological Age

Save to myBoK

by Suzanne Schoenfelt

Are smart cards a viable solution for storing patient information? What about companies that store and provide emergency medical information? The author examines the possibilities these services offer.

These days, wallets are bulging with a proliferation of cards. Issued from grocery stores, video stores, gas stations, airlines, insurance companies, banks, places of employment, and the library, the cards serve myriad purposes. Most of them are likely to be magnetic stripe cards. (The stripe stores information much like audio tape.) Other, more technologically sophisticated cards store greater amounts of information. These "smart cards" are embedded with a computer chip, and—in some cases—even an on-board microprocessor, erasable memory, and operating system. Anything that can be digitized can be deposited into the chip and stored on the card: identification data, stored monetary value (for example, phone cards), even biometrics (a physical characteristic that identifies an individual).

Smart Cards for Storing Medical Records?

Smart cards present an interesting technological option for carrying, storing, and accessing medical information. In simple form, a smart card (or patient card) provides identification information, such as name, address, date of birth, and perhaps authorization for payment. A broader use may involve a patient's lifetime medical record (including risk factors, allergies, medications, test results, medical treatments and responses, and family, social, and medical history), communication among healthcare providers, data storage, and access control to health information.

Technology, while able to solve complicated problems by simple and inexpensive means, often raises equally complicated issues. Smart card technology makes information more accessible and, by extension, reintroduces questions of confidentiality, security, and release of information.

Does more accessible mean less secure? According to some industry sources, not necessarily. Others are dubious. Medical information, governed in the US by confidentiality and privacy laws, needs to be protected. Adopting smart cards for storage of medical histories would not merely convert paper files to electronic ones—it would change the form of recorded medical information.

Current Methods: Companies That Store Patient Medical Information

Many companies provide storage of essential medical history where data can be accessed (by phone or by fax) 24 hours a day, seven days a week, from anywhere in the world. The oldest and probably best known of these organizations is Medic Alert, a nonprofit company that has existed since 1956 and whose emergency medical identification emblem is recognized worldwide. A Medic Alert member wears the emblem on a bracelet or necklace. On the identification is engraved the name of the wearer's medical problem, membership identification number, and the Medic Alert 24-hour central telephone number by which healthcare providers can access more detailed information. (Members also carry a wallet card with medical information inscribed on it.) This service is especially valuable to people whose chronic conditions are not easily recognized in emergency situations.

According to David Roth, communications director at Medic Alert, the company has no plans to implement smart cards. "We don't feel a smart card is fitting for emergency situations," Roth comments. "Standard emergency operating procedures do not involve searching for wallet cards or any other ID. Medic Alert works with EMS responders in the way they work."

Roth adds that what a medical response team commonly wants Medic Alert to provide is a small data set containing medical records that are most pertinent to patients in an emergency situation. "The Medic Alert ID bracelet contains the most important medical facts, such as drug allergies or whether a patient is insulin dependent or prone to grand mal seizures," he says. "Medic Alert's emergency response center transmits medical files (a small subset of a patient's medical history, meaning vital medical facts that could most significantly affect a patient during an emergency)."

The body-worn bracelet is simply an alerting device, Roth says. "This is what paramedics are trained to look for. Emergency personnel are advised not to look through wallets and purses. More significantly, in accident situations, a person can easily be separated from possessions. That's why the body-worn ID is the best method of conveying information immediately in emergencies."

Other companies function in much the same fashion as Medic Alert. Members file medical information with a company, sign a release authorization, and carry an identification card with access instructions that include a toll-free number. For members of Lifefax, a caller is directed to an automated system. People on the emergency scene are automatically able to access the patient's medical file, again with the use of a phone and fax machine.

Candidates for the service include seniors, those with complicated medical backgrounds, travelers, people away from their normal support structures, and college students, according to Byron Burpulis, executive vice president of marketing and sales of Lifefax. The depth and breadth of medical information registered with the service is up to an individual member. Files might contain scanned picture files, prescriptions, EKG trends, passports, as well as advanced directives such as living wills and donor information, Burpulis says. Members are allowed to include any and all attachments.

Regarding security measures that protect information, "the patient makes the moral and ethical decision about what information should be released by deciding what information to provide," Burpulis says. "Anyone can dial the company's access number on a patient's card, go through a chain of commands, and have the information delivered. Even a morning jogger can potentially help a person in a medical emergency. The company puts the control of confidentiality totally in the hands of members."

Another company, Medifile, provides a similar personal health record service for consumers in which members provide information that is stored in a database, sign an authorization for release, and carry an access card with instructions for release of information in both emergency and routine circumstances. "Information is released only to authorized healthcare providers," says Diane Brooks, assistant manager. "When a caller requests information from Medifile, the name, location, direct telephone number into the emergency room, as well as the provider's main telephone number are required. In addition, Medifile is adding a new feature to its service whereby this information will be cross-checked against a database of providers. Medifile telephones back through the provider's main number." The whole process takes about 15 minutes, Brooks says. All employees of Medifile also sign a nondisclosure agreement agreeing to handle sensitive member information with confidentiality.

Security: Is the Smart Card Really Smart?

No matter how information is stored, security is an issue. Two prominent threats to patient security are insurance companies interested in being privy to patients' medical conditions and pharmaceutical companies interested in databases for marketing purposes.

But Dan Cunningham, president and CEO of the Smart Card Industry Association (SCIA), says smart cards are orders of magnitude more secure than other available technology. "Even if you could increase the level of privacy and security, the technology is always susceptible to hackers," Cunningham says. "But this is true of any security system. You have to figure out how to detect problems and how to react."

Information on a smart card can be protected by a PIN or by biometric stored in the card itself, he said. "If a cardholder wants certain information restricted from viewing, the information can be stored in the card in such a way that it can't be accessed. Security can also be devised so that providers have different PINs, making different information available to different providers."

Even though optical cards have the advantage of high-capacity storage capability over chip cards, the disadvantage is security, Cunningham says. "Anyone can read information on an optical card." The data on optical cards also tends to be corrupted by

marks on the card's surface. And the read-write devices needed for optical cards are more expensive (e.g., $1000) than the devices needed for chip cards (e.g., under $100).

Cunningham estimates that last year, more than 1 billion cards were manufactured worldwide for various uses across all industry applications. But smart cards are still not as widely used in the US as they are in other countries. Cunningham attributes this to certain features of the American economic and business infrastructure. "We have a very cost-effective telecommunications infrastructure," he says. "We do not have a concentration of business firms capable of dominating a particular market segment as some countries do. The US public telephone market is highly fragmented, making it impossible for a handful of firms to implement a nationwide prepaid telephone card. (In many countries, the public telephone system is state owned or licensed.) And our culture is different. In the US, people are more concerned about privacy. If the German government decides to issue a healthcare card, people simply use it."

Lack of exposure and knowledge is another reason smart cards have not been used more widely, believes Christy Roberts, RRA, who served as AHIMA's staff liaison to the Health Identification Card Technical Advisory Group of the Workgroup on Electronic Data Interchange in 1993. "Many healthcare organizations are still working to achieve system compliance for the year 2000," says Roberts, now director of HIM at Springhill Memorial Hospital in Mobile, AL. "Additionally, most rural healthcare providers and hospitals still have systems that are not current with technology's ability. The major reason is lack of funding." Roberts believes the main goal in applying smart cards for everyday use in the healthcare system should be ensuring that the cards are secure mechanisms and that information is not released inappropriately.

Smart Card Technology in Use

Smart card technology is already widely used in the healthcare systems of Germany, France, and Spain. Europe adopted the technology because the region lacked electronic data interchange and telecommunications systems necessary to provide easy access to centralized databases.[1] In Germany, which has a national healthcare system, 80 million cards have been distributed to citizens. The cards carry primarily administrative data, such as name and address, and hold only 2000 bits (256 bytes) of information. When a patient visits a healthcare provider, he or she presents a card that is electronically "read." Information is plugged into a claim form electronically, eliminating the need for filling out forms, re-keying database information, and other administrative functions. France is introducing a more complicated health card, and Spain is in its second year of using a combination social security and healthcare card.[2]

France's card is considered secure and almost impossible to hack. If a French cardholder disagrees with information on the card, the system will destroy the card. (The cardholder re-files information.) The system allows only four tries for access. On the fifth try, the card self-destructs. Dismantling the card to remove the chip destroys the data.[3] Australia and Japan have also implemented studies of smart card technology.[4,5] In Taiwan, an optical card is used for insurance information.

In the US, the cards are in use in business sectors but have yet to be used widely in the healthcare industry.[6] A variety of projects have been undertaken, however, by the US military. The most recognized for healthcare information is a pilot program of the multi-technology automated reader card (MARC), a smart card[7] and a potential storage device of casualty medical information for use during combat. MARC (used with MEDTAG, a hand-held portable electronic unit designed to use MARC to store medical data) was tested by medics of the 25th infantry division in Oahu, HI. The MARC system demonstrated improvements in speed, documentation quality, and user satisfaction over the paper field medical card historically used to document clinical records of those injured in combat.

In combat, medical personnel typically have limited knowledge of a patient's status. With the MEDTAG concept, all military personnel carry their own medical data on electronic media. Its efficacy saving lives during combat—the most important measurable variable—has not been assessed. As far as security goes, however, MARC does not allow access between functional areas (for instance, between a demographic record and a medical record).

smart cards at home and abroad

- **1993**: The Florida Medicaid system phases in a card as a key to a data base. When the provider swipes the card with the information about the payer and enters the date of service, the card reader sends a signal to a Medicaid eligibility verification vendor, which in turn sends a signal to Florida's Medicaid fiscal agent. The fiscal agent verifies eligibility and replies about a patient's eligibility as well as other health insurance coverage through an online, real-time system. The answer comes back in 15 seconds. This system also has eliminated the cost of mailing one million paper eligibility cards every month and change of address problems.[8]
- **1995**: An Australian study shows how the smart card memory can be zoned into different security levels. For instance, the highest-level security zone contains an individual's full medical history, and the lowest security zone contains the cardholder's name and address. Different zones can be made more secure.
- **1996**: A German study successfully applies smart card technology (DIABCARD) for chronic diseases, specifically diabetes, in ambulatory and hospital care.
- **1996**: Japan establishes an off-line network system of health and welfare for elderly people using optical memory cards. The system covers almost one-third of people over the age of 65 in a designated city and almost all of the offices concerned with their health and welfare. The optical memory card holds basic data for health and welfare, health check information over a five-year time span, medical images, and history of welfare services. All the data are used for medical care, health consultation, and management of health and welfare services.
- **1997**: The State of California issues 5 million stripe ID cards to Medicaid patients. Though the initial investment is significant (the state had to spend $34 million building the network), the state saves about $2 million per year in card costs. (The state no longer needs to mail recipients 5 million paper cards each month.) The state predicts another $25 million per year in savings through efficiencies gained, primarily through labor and fraud reduction.[9]

Issues of Standardization

In the opinion of Peter Waegemann, executive director of the Medical Records Institute and chair of the International Patient Standards Council, the application of cards for patient data has not been very successful. Waegemann says that one of the downfalls is that in many cases, most information is available to update a patient's card only after the patient has left a physician's office. Problems with record storage won't be completely resolved until medical records systems are standardized, says Waegemann, who also chairs the ANSI Healthcare Informatics Standards Board and the US TAG for ISOTC215 Technical Committee on Health Informatics.

As health information technology continues to develop, Waegemann believes, the smart card will similarly evolve. In the future, smart cards may evolve not as patient cards, but as health professional cards, he says. A healthcare professional could use the card technology to access patient information from a database. "This is a more secure and efficient way of handling information," Waegemann says. "The reality of the future will probably be that, rather than searching for cards in a patient's wallet or on a patient's person, information will be downloaded over the Internet. That is cheaper and faster."

table 1—picking the right card

Types of Cards	*Characteristics*	*Storage Capacity**	*Costs to Produce*[10]
Magnetic Stripe (used commonly for credit cards)	Like audio cassette tape, the stripe can be read, copied, edited, or deleted by anyone with the proper device.	Data can be coded on three lines: tracks 1, 2, and 3 totaling a storage capability of 226 characters of information.	$.10
Smart Cards (Chip Cards)	A chip is stored in the card. More reliable, performs multiple functions. May be embedded with microprocessor, erasable memory, operating system. More secure because of high-security gatekeeper mechanisms such as advanced encryption, password, pin, and biometric protection. Authorized readers may view different levels of data, depending on level of authority.	These cards allow thousands of times the information storable on magnetic stripe cards. Capable of carrying as many as 20 pages of information.	$3-10
Optical Cards	Use CD-ROM-like laser engraving to permanently store large amounts of data. High-end cards that can store complex test results, such as MRIs. No security mechanism.	Capable of carrying as many as 2000 pages of (up to 4 megabytes[11]) information as well as large files such as ultrasound results and digital photos.	$5 (or more)

*Storage and cost figures were taken from the *Health Data Management* publication.

Notes

1. McCart, Alice. "Patient ID Cards: Passports to Care." *Medical Claims Management* 2 (1993): 57.
2. Cross, MargaretAnn. "Assessing the Role of New Card Technologies." *Health Data Management* 5, no. 4 (1997): 58.
3. McCart, p. 58.
4. Morris, S., J. Cooper, D. Bomba, L. Brankovic, M. Miller, and F. Pacheco. "Australian Healthcare: A Smart Card for a Clever Country." *International Journal of Biomedical Computing* 40, no. 2 (1995): 101-5.
5. Sakashita, Y., Y. Ogushi, Y. Okada, M. Horie, Y. Ohta, Y. Hayashi, S. Suzuki, Y. Haruki, and T. Takahashi. "Health and Welfare Data on Optical Memory Cards in Isehara City." *Medical Informatics* 21, no. 1 (1996): 69-79.
6. Cross, p. 58.
7. Konoske, P.J., R.W. Dobbins, and E.D. Gauker. "MARC ES: A Computer Program for Estimating Medical Information Storage Requirements." *Military Medicine* 163, no. 1 (1998): 49-55.
8. McCart, pp. 57-58.
9. Cross, pp. 62-64.
10. Cross, p. 69.
11. McCart, p. 57.

References

Appleby, Chuck. "Retro Tech." *Hospitals & Health Networks* 69, no. 5 (1995): 40-42.

Brandt, Mary. "Position Statement: Patient Cards." *Journal of AHIMA* 64, no. 11 (1993): insert.

Chidley, Elise. "New Patient Card Links to Partial Electronic Medical Record." *For the Record* 9, no. 14 (1997): 24-25.

Engelbrecht, R., C. Hildebrand, E. Brugues, A. De Leiva, and R. Corcoy. "DIABCARD—An Application of a Portable Medical Record for Persons with Diabetes." *Medical Informatics* 21, no. 4 (1996): 273-82.

Eve Mitchell, "Emergency Card Gives Any Hospital Fax Access to Holder's Medical History," *The Fort Worth Star-Telegram*, 13 April, 1997, p. 4.

"New Jersey 'Smart Card' on Deck." *AHA News* (March 4, 1996):6.

Pangalos, G. "Design and Implementation of Computer-readable Patient Data Cards—Applications in Europe." *Medical Informatics* 17, no. 4 (1992): 243-256.

Roberts, Christy. "Report on the Activities of the Health Identification Card Technical Advisory Group (TAG) of the Workgroup of Electronic Data Interchange (WEDI)." *Journal of AHIMA* 64, no. 11 (1993): 66-69.

Suzanne Schoenfelt *is owner of The WordSmith, a medical, scientific, and pharmaceutical communications service in the Chicago area.*

Article Citation:
Schoenfelt, Suzanne. "New Possibilities for Patient Information Storage in a Technological Age."*Journal of AHIMA* 69, no. 8 (1998): 50-54.