The Smart Indian Soldier

Lieutenant Colonel Sunil Jain, MD*

Introduction

With the launch of "Universal ID Authority of India" Project, the idea of unique identification number has caught the fancy of Indians. The Indian Armed Forces have had this system in place for many years. This is being done in a well organised manner. However, advances need to be brought in information technology to the Armed Forces in a scientific manner, to facilitate foolproof identification, and maintenance of service / health records.

The smart cards have been introduced in the Armed Forces for availing CSD facilities. It is said that army marches on its stomach. But in modern adage it will be said it advances on 'spices'. Change is the spice of life, and change for scientific advances incorporation is the need of the hour. The smart cards should be introduced for health purposes first, and the healthy troops will thus march to victory.

The Need

The two important needs of the Armed Forces are 'identification' and 'dynamic record keeping'. A Smart Card can fulfill both these needs with one card. It would replace a variety of other documents used for maintaining personal data and records. It would also be amenable to upgradation periodically with advances in technology.

Smart Card ID - Introduction

A Smart Card includes an embedded computer chip which can be either a microprocessor 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 mutual authentication) and interact intelligently with a Smart card reader. A Smart card ID can combine with several ID technologies, including the embedded chip, visual security markings, a magnetic strip, a barcode, and/or an optical stripe.

Smart cards are used worldwide: in financial, telecommunications, mass rapid transport, for secure identification to control access to buildings and offices, as administrative tools for students in campuses, in healthcare and other applications.

Secure Identification

One of the main purpose of Identity cards in the Defence Forces is to verify the identity of individuals seeking access to specific locations. The futuristic needs would call for a wide range of applications – from enabling access to facilities or secure networks, to proving an individual's rights to services, virtual record keeping and for conducting online transactions.

Integrated Biometric and Smart Card technologies will provide almost foolproof security. Biometric technologies are defined as automated methods of identifying or authenticating the identity of a living person based on unique physiological or behavioural characteristics. Smart cards have the unique ability to store large amounts of biometric and other data, carry out their own on-card functions, and interact intelligently with a smart card reader. Secure ID systems that require the highest degree of security and privacy are increasingly implementing both Smart Card and Biometric technology.

There are numerous government ID systems implemented worldwide that are using Smart Card and Biometric technology. These include :-

(a) US Department of Defence Common Access Card - with photo, biometrics (fingerprint) and a smart card chip. This is one of the most advanced ID smart card programmes. The Common Access Card (CAC) serves as the DoD (Department of Defence) standard identification for active duty military personnel, selected reserve personnel, civilian employees, and eligible contractor personnel. The CAC is the principal card used for logical access to DoD computer networks and systems, and will be the principal card used to enable physical access, as systems are installed for authentication and access at DoD facilities. As of May 2008, DoD had issued over 12 million Smart Cards. As with all Federal agencies, DoD is now migrating to a FIPS 201-compliant Common Access Card.1

(b) Netherlands' 'Privium' automated border crossing system - with photo, biometrics (iris) and a smart card chip.

(c) Malaysia's National ID (Government Multi-Purpose Card) - with photo, biometrics (fingerprint) and a smart card chip.

Selecting a Biometric Technology

Biometrics can provide very secure and convenient authentication for an individual since they cannot be stolen or forgotten and are very difficult to forge. The two types are:

(a) **Physiological characteristic** – These are relatively stable physical characteristics, such as an individual's fingerprint, hand geometry, iris pattern, retinal pattern etc. This type is usually unchanging and unalterable without significant duress to the individual.

(b) **Behavioural characteristic** – This is more a reflection of an individual's psychological make-up. A signature is the most common behavioural biometric used for identification. As most of the behavioural characteristics vary over

time, an identification system using these must allow updates, to enrolled biometrics references.2

Table 1 shows a comparison of different biometric technologies with their performance rated against several metrics.3

Table 1 : Comparison of Biometric Technologies

Characteristics	Ease of use	Error incidence	Accuracy	User acceptance	Long term stability
Fingerprints	High	Dryness, dirt, age	High	Medium	High
Hand Geometry	High	Hand injury, age	High	Medium	Medium
Retina	Low	Glasses	Very high	Medium	High
Iris	Medium	Lighting	Very high	Medium	High
Face	Medium	Lighting, age, glasses, hair	High	Medium	Medium
Signature	High	Changing signatures	High	High	Medium
Voice	High	Noise, colds	High	High	Medium

Memory Use

Biometric systems store either the full biometric image or a biometric template. Biometric templates are small, ranging from nine bytes for hand geometry to 300-1200 bytes for fingerprint scan to 512 bytes for iris recognition to 1500 bytes for voice verification. Smart cards have sufficient on card memory to store one or more biometric templates.

The Impact

These technologies will have a tremendous impact for security purposes. Only genuine persons will be able to enter the sensitive areas. This will obviate the need of sentries in many areas and the need for oral passwords. Thus, there will be a saving on manpower and money.

Electronic Medical Records – Evolution and Miniaturisation

Lack of medical data can lead to inefficient or inappropriate practice.4 Also it can lead to essential care being delayed or withheld. An intervention that addresses even a fraction of this problem will have many financial and clinical benefits.5 The electronic medical record was introduced in an attempt to solve this issue. The medical records should be available on all hospital terminals,6 and in our set-up at all Field aid posts, Field hospitals and other hospitals.

Medical record keeping has used new technologies, developed by using globally accepted standard platforms such as HTTP, HTML and the internet. The scope of use was ambitious. Further these systems are compliant with security requirements for the confidentiality of electronic health data published by the US National Library of Medicine.7 However, concern about breaches in internet security is a threat and it may violate patient confidentiality. Importantly in health care, security of data and confidentiality are generally recognised as being pillars of ethical practice. Smart cards offer a ready made solution to some key problems of security and confidentiality.8

It is imperative that the medical records should be carried by the patient and given to doctors whom they desire and wherever they desire. This again has led to smart cards being considered as a possible solution. The low cost of the cards, their increasing storage capacity, and the fact that patients carry their card to the point of care make the smart card an attractive option. This will serve both the purposes i.e. as identification token and as a data container.

For privacy and security reasons the contents of the smart card will be accessible only by a doctor’s PIN coded key card.9

Past History / Medical Records – Importance Revisited

It is highly important in any medical consultation and especially in emergency situations that past medical history is readily available. This should contain blood group, allergies, personal medical history, ailments, medications, immunisation details, family medical history, and health schedules.

A lot of morbidity and mortality due to drug interactions, allergic reactions or misdiagnoses can be prevented if medical professionals and care givers have access to proper medical records. Many times the information is inaccessible, inaccurate, lacking in detail or out dated. Accessing certain vital medical information makes the difference between life and death in an emergency situation.10

Further, a smart card can store all medical reports including laboratory diagnostic data, radiography, ECG, ultrasound imaging, CT scans, MRI and morphologic slides.

In lighter vein

With the widespread worldwide use of electronic health records the chapter on “past history taking” in the renowned Hutchison’s Clinical Methods will either become history or will be shortened. It might be replaced by how to record and read electronic health records!

Smart Cards & Combat Zone

Medical data available in emergencies can be life-saving. Small and portable technology of Smart Cards allows them to be carried to the forward most location.

For fighting fit troops in the combat zone, medical records including physiological characteristics, are important and imperative. Knowledge of the physiologic parameters, which provide a more objective measure, may decrease mortality in combat casualties.11

In emergency management of combat injuries, blood group is one of the most important of all medical records. The leading cause of death on the battlefield is uncontrolled hemorrhage.12 Policies allow the use of identification cards and tags for transfusion purposes during contingency operations.13 Blood transfusion hazards persist and include human errors resulting in the inadvertent transfusion of incompatible blood.14 Blood group tags on combat uniforms can have various errors. Typographical errors in blood group lists maintained in units/contingents and individual paper cards can be disastrous. These factors make error reduction a priority and medical records on smart cards emerge the best option.

The role of Army Medical Corps has a long road. This can be simplified with supportive technology. Smart cards are useful both in life and death. For the second eventuality, use of Smart Cards with biometric technology can be useful and decisive.

In future the biometric technology should also include dental characteristics. Forensic dentistry is important to the armed forces.15

Medical Boards: **“From opinion to disposal” - the Smart / Electronic way**

The specialist will punch in his opinion in a preformatted Performa, will encrypt it on the Smart Card and simultaneously forward it to all concerned, including the Records office, via the intranet.

As regards to privacy and confidentiality, electronic data can be better secured than paper records, because authentication, authorisation, auditing, and accountability can be facilitated.16

The use of an Electronic Medical Record (EMR) system may overawe most users at the beginning, but once a comfort level is established, EMR is likely to outscore conventional paper recording systems.17

The Impact

Introduction of Smart Cards will impact and facilitate following aspects :-

(a) Were smart cards adopted for the storage of medical histories it would change the form of medical information recorded, not merely convert paper files to electronic ones.18 It will become more systematic.

(b) Collating of data will become easy and trends visualised instantly for immediate policy action.

(c) Electronic data can be better secured than paper records, because authentication, authorisation, auditing, and accountability can be facilitated.

(d) Continuum of care: It has been aptly said “Once a soldier always a soldier”. The information stored on Smart Cards can be of continued use even after retirement. The Smart Cards will allow easy extraction and prevent duplication of efforts for pertinent information.

(e) This will result in tremendous cost cutting and cutting of trees for paper. The Army Postal Service (APS) would become more efficient and may have additional responsibilities.

Personal Data and Records

There is sufficient memory for recording these in the Smart Cards.

The Current Scenario

Internationally, a few examples of countries using Smart cards are as under :-

France - SESAM Vitale: One of the biggest e-Health schemes in the world and also one of the most successful. Up and running since 1998, the SESAM-Vitale system links healthcare professionals with the compulsory health insurance administration. Version 2 of SESAM-Vitale, which is currently being deployed, offers the current standards in terms of security and will enable stronger identification of social security beneficiaries.

The Carte Vitale 2 will not just allow for a simplification of administrative procedures, increase transaction security and speed up reimbursements, but will also contain considerable additional information like details of attending physicians, people to contact in case of emergency, authorisations for organ donation and top-up insurance policy details. Furthermore, the Carte Vitale 2 will include a photograph of the insured person that conforms to the latest Identification, Authentication and Signature (IAS) specifications19.

German Health Care Card: One of the largest IT projects in the world. Total of 71 million people now carry the card.

Supports cryptographic capabilities for digitally signing medical documents and prescriptions.

The Taiwan's Bureau of National Health Insurance: To help control (contain) costs, facilitate electronic claims and improve healthcare quality, Smart cards have been deployed nationwide. So far, 23 million patient health cards and 345,000 healthcare professionals (providers) cards have been issued.

In India, *Rashtriya Swasthya Bima Yojana,* launched on October 1, 2007, is using Smart cards for cashless transactions for health care. It covers all workers in the unorganised sector who come in the category of Below Poverty Line (BPL) and their families. The advantage is – if users migrate they can use the smart card wherever they go.

Conclusion

A number of private players are vying for the use of Smart cards in Healthcare. They also want the UID number to be linked to a UHID (unique healthcare identification number). In India this should be first done in a well organised manner in a well managed group i.e. the Armed Forces. Subsequently, the same can be done for all the Indian nationals. The experience of the Armed Forces in the form of systematic and secure functioning will be of great utility. The Armed Forces, already entrusted with the Nation's security can secure data the best - in healthcare and other selected areas as well.

***Lieutenant Colonel Sunil Jain,** MD is a classified specialist (Paediatrics), MH Saugar.

Journal of the United Service Institution of India, Vol. CXLI, No. 583, January-March 2011.