Role of Biometrics in healthcare privacy and security management system

Dr. G. D. Mogli Ph.D., FHRIM (UK), FAHIMA (USA)
Sr. Consultant eHealth Management, HEARTCOM INC. (USA)
E-Mail address: gdmogli@yahoo.com www.drmogliit.com

Sri Lanka Journal of Bio-Medical Informatics 2011;2(4):156-165
DOI: http://dx.doi.org/10.4038/sljbmi.v2i4.2245

Abstract

Introduction
Healthcare system which is in the process of transformation to provide swift, safe and improved quality care is experiencing multifarious problems. In the process, the computer network is playing a very vital role and its implementation has contributed enormously but there are problems too, eg. passwords that are meant to protect computer network systems from unauthorised use which however may also provide a false sense of security. Some use easily guessed passwords, thus facilitating unauthorised access. Patient records are vital for patient care, but incomplete health records or misplaced information or mix ups with another patient's record can result in wrong medication. In addition, if the records are in the wrong person's hand, it can lead to a great hazard to a patient's health.
Why Biometric?
Biometric identification systems employ the use of biological data, in the form, of voice, face and signature scans. The most common physiological biometric include finger-scan, retina scan, hand-scan, and iris-scan. Biometric identification cannot be forgotten or stolen and involves the use of IT to acquire, analyse, store, manage and transmit genetic data. Since April 2009, in the US, Health Insurance Portability and Accountability Act (HIPAA) require physicians and healthcare professionals who use Electronic Health Record (EHR) track to be tracked every time a patient's record is accessed. Generally, one could digitally authenticate a user with any of these authentication methods: "what you know, what you have, what you are or who we are" refer to what is unique about us, our physical bodies as human beings. Things like fingerprints, retinal design, facial shape, vocal wave, hand geometry and in the future, DNA. Authentication is referred to as 1:1 (one-to-one) matching.
Ethics in health informatics
Biomedical ethics address issues such as privacy and confidentiality, conflicts of interest, harm to patients and the nature of the relationships between the physician and the patient which need to be balanced between potential harm and benefits of use of IT.
Bioterrorism and Public Health
Biometrics is very helpful in two ways. Firstly, the biometric identification of terrorists can be distributed electronically to all potential risk areas within and outside the nation for preventive purposes. Secondly, it can help in detecting the disease and if effective, would substantially reduce the mortality and morbidity with the early warning system detection of surreptitious biological attacks.
Conclusion
Biometrics play a very vital role in not only in maintaining privacy and security of healthcare management system but also in bioterrorism and public health activities in notifying infectious diseases and controlling mortality and morbidity rates by linking with curative medical facilities.

Keywords - unauthorised access; identification system; biological data; physiological biometric; privacy and confidentiality

Introduction

The healthcare system, in the process of transformation to provide swift, safe, improved quality and cost contained care, is experiencing multifarious problems. To specify a few, passwords that

are meant to protect computer network systems from unauthorised use, may however provide a false sense of security. Another aspect is the use of health records that get mixed up, are incomplete or which contain misplaced information and wrong medication. This may sometimes lead to transfer of one patient's information into another's record. Furthermore, records may pass to a wrong person despite many security measures.
Security issues arise because people forget or share passwords or write them down, stick on monitors and even store them on or near the computer. Some use easily guessed passwords, thus allowing unauthorised access to entire computer network systems. Furthermore, 60 to 80 % of workers disclose their passwords to a colleague if asked. Many people actually write passwords on "post-it" notes and stick them to their computer screens or keep under their keyboards. On the other hand, passwords, personal identification number (PIN), smart cards can be easily obtained or even shared. The same security breach can happen with patient confidentiality and patient medical records.

Research facts on passwords problems

The following information is being quoted for its authenticity and importance. The Gartner Group reports that 40% of all help desk calls are for forgotten passwords. Each year, companies spend up to USD 150 per user trying to maintain secure passwords. Up to 15% of annual IT budget is spent on information security. Despite firewalls, encryption and other safeguards, many IT professionals who are bent on creating a secure information system, fall short because ultimately, the network can easily be compromised when an authorised user shares his or her password.

Current solutions for the password dilemma only aggravates the problem. Rules call for longer strings of letter and number combinations, frequent password changes, and multiple passwords, making it more challenging to comply with security because the new requirements are difficult to follow. Attempts to make passwords more secure require them to include a specific number of characters and to contain a combination of letters, numbers, and symbols; and to change them frequently. Having access to each application controlled by a separate password, make memorisation mandatory. "Passwords are not absolute. The swipe of a finger on a laptop or other peripheral can substitute for several passwords" says Victor Lee, a senior consultant for the International Biometric Group.

Password protected

Most industries concerned with security have used passwords or PIN numbers for protection of their private and confidential information. These passwords are usually simple to remember and very often the same password is used for every system. Unfortunately, passwords can be compromised or "traded" and therefore true accountability is lost. This is true for the activities in the emergency department as well. A physician prescribing narcotics that uses a password based system can be watched, the password written down and duplicated with little difficulty. The same security breach can happen with patient confidentiality and patient medical records. Because of the inherent weakness of password systems, other identification systems have been developed.

Why biometrics?

There is an anxious race going on to find the best method of securing healthcare data and preventing mistakes which are considered to be very serious. Despite the financial burden, more healthcare organisations are turning to biometrics as a means to increase security, privacy and improve patient safety. The biometric is a solution to the Health Insurance Portability and Accountability Act (HIPAA), and many such laws worldwide need such a mechanism to guarantee a patient's privacy. Biometrics is making it possible for patients and healthcare professionals to feel secure that their information is being kept confidential and is only being released to those who have the right to see it.

Since April 2009, the US requires that physicians and healthcare professionals who use electronic records be tracked every time a patient's record is accessed. Biometrics allow the physician to do this easily. By making the records only accessible to someone who is identified via hand/thumb/iris print, a record can be kept of who accessed the files and when, and it can be ensured that the person who accessed the file is definitely who they say they are and has the right to see a patient's record. If they mismatch, the appropriate authorities can be notified that someone without authorisation is trying to access secure data.

Biometric identification system

Biometric identification systems employ user's biological data, in the form, for example, of voice, face and signature scans. The most common physiological biometric include finger-scan, retina scan, hand-scan and iris-scan. The Iris Technology was developed on 18 February 2002, by the University of Southern Alabama Medical Centre (USAMC) which became the first acute care facility to implement Iris Scan Technology for system access control and user authentication. In fact, iris scanning is reputed to have an error rate of only1 per 1.2 million scans. Iris-scan can verify or identify a person based on the unique characteristics of the human iris. The strengths of iris-scan include its high resistance to false matching, the stability of the iris over time and the ability to use this biometric to provide access to healthcare information or entry into a physically secure location, such as a medical record keeping or Information Technology Department. Biometric identification is superior to passwords in two ways. They cannot be forgotten or stolen. Bioinformatics involve the use of IT to acquire, analyse, store, manage and transmit genetic data. In the future, gene chips will be used to acquire genetic data; data mining will be used to extract data from large databases and warehouses. Decision support systems will be used to analyse data and to make clinical decisions. Because biometric security is based on a unique feature of an individual's body, for instance, it is very difficult to copy, steal or replicate a fingerprint. The strengths of finger-scan are that it is already a proven technology that provides high levels of accuracy. It can be deployed in a wide range of environments (desktop, keyboards, mouse, PDAs, laptop, provides physical access to information storage facility), it is easy to use and users can enroll multiple fingers for verification and authentication. The final biometric that could gain wide use in the healthcare sector is the hand-scan. This biometric uses the unique aspect of the human hand, specially the height and width of the back of the hand, to verify and identify an individual. The hand-scan can be used to provide physical access to highly secure areas and monitor when an individual arrives and leaves the workplace.

The strengths of this technology include its ability to be used in different environments, reliability and convenience. Drawbacks are the cost and limitations in applicability. In terms of future use, look for the finger-scan to be the most widely accepted biometric by healthcare industry.

The biometric devices consist of a reader or scanning device, software that converts the scanned information into digital form, and a database that stores the biometric data for comparison. IBM, Microsoft, Novell, and other computer companies are currently working on a standard for biometric devices, called BioAPI. This standard will allow software products from different manufacturers to interact with one another.

Smart cards vs. Biometrics

Compared to smart cards, the ultimate promise of biometrics is twofold. Firstly, biometrics tie authentication to an actual user, instead of a private key or token the user possesses. Secondly, it frees the user from having to remember or carry anything.

What are the risks?

The best, one could ever hope for is a high degree of likelihood. For instance, a typical fingerprint scanner will grant unauthorised access to one of every 1,000 illegal attempts to enter. This is known as false acceptance rate (FAR). Beyond security, privacy is a major issue for biometrics. The risk associated with a potential identity compromise is a thousand times greater than with a password, certificate, or smart card. Yet another risk shared by all means of authentication methods is that of replay. Even the most sophisticated PKI will always rely on the transmission of private keys. These keys are no different than passwords. They can be stolen and used to intercept sensitive documents or forge signatures. In biometrics, the risk of replay is just as real, and must be adequately addressed in any secure user authentication scenario.

Future of biometrics

Everyone recognise that human lives depend on shared medical data and information and any effort to effectively share information requires a trusted health data exchange. Security is always a vital concern when it comes to confidential medical data and must be balanced with convenient access to patient records. Another key issue for adoption of biometrics is privacy which is of paramount importance. It is fair to say that any biometric solution that implants an actual physical identifier in a patient record, such as ‘bitmap of a patient’s signature, must adhere to stringent regulatory requirement that protect the patient’s privacy in the event of compromise.

A natural solution

Finger scan technology is the most common biometric authentication technology used by millions of people worldwide because of its low cost. This is well known in forensic applications. Finger Scan Technology is steadily gaining acceptance in fields as varied as

banking, physical access, network security, public services, e-commerce, and retail. Employing fingerprint clearance not only prevents fraudulent prescriptions from being written, but provides an audit trail for reducing the liability exposure of the hospital and physician.

Biometric devices and record security

A staff member walks up to the file room door, places his hand on the shiny glass panel, and in an instant the lock clicks, the door opens and a digitised voice says. "Good morning, Mr. Peter". Sound like the opening scene of the latest James Bond movie? It could be, but the fantastic vision of filmmakers is becoming more commonplace than one may think.

Two-factor authentication

Generally, one could digitally authenticate a user with any of these authentication methods such as what you know, what you have or what you are.

What you are: Now we get to biometric authentication. "Who we are" refers to what is unique about us, our physical bodies as human beings. Things that can be measured, stored, and tested against. Things like: fingerprints, retinal design, facial shape, vocal wave, hand geometry and soon DNA. However, we cannot forget that in order to be effective we still need to deploy two factor authentications. For example, these could include either a user name (what you know) and a fingerprint (what you are) or a pass card (what you have) and a facial scan (what you are). This compensates for the fact that no biometric technology is perfect.

Getting started with biometric authentication

From the beginning biometrics has been recognised as a tool. Does an employer have a strategic initiative that would receive benefits from biometrics? Could this technology help support HIPAA compliance? The answer to both these questions is a definite "yes". Could biometric increase security? Yes, and No. Once the need for biometric authentication is established and supported, one needs to consider the options (in some ways simultaneous with established need). What kind of scanning option is right for the given environment? One may discover that more than one type is needed; such as finger scan and iris or voice etc.

Ethics in health informatics

The rapid growth of bioinformatics presents additional, social and ethical issues. Acquiring and using genetic data for clinical purposes will raise issues concerning consent and appropriate use of these data. When there is no treatment or cure for diseases that have a genetic origin, would most patients prefer not to be told about the results of genetic testing? Who can appropriately access and use patient-specific genetic data? Should certain uses of these data be prohibited? For example, insurance companies may use this information to determine eligibility for coverage and employers may use it to hire and assign employees to specific jobs.

Biomedical ethics provide a common frame of reference to address cases such as privacy and confidentiality, conflicts of interest, harm to patients and the nature of the physician-patient relationship are fundamental and implant the healthcare system of any country. Ethics help to

identify issues that involve questions or right or wrong, appropriate or inappropriate actions on the part of individuals and organisations. For example, when, if ever, is it ethical to sell or use private patient medical information for commercial purposes such as marketing pharmaceutical products?

Often there needs to be a balance between potential harm and benefits of uses of IT. One way to assess these issues and resolve conflicts is to establish institutional ethics committees. Members of these committees can also serve as consultants when issues arise. In fact, the Joint Commission on Accreditation of Healthcare Organisations (JCAHO) requires accredited organisation to establish a mechanism for addressing ethical issues. Another way that bio-ethics can contribute to medical informatics is by contributing to the development of professional standards.

Advantages of biometrics

With biometrics security, physicians only have to log-on once and then they have access to laboratory results, CPOE, and the radiology database. Furthermore, a hospital network can be biometrically protected, thereby protecting sensitive information from attacks by "war drivers" and other hackers. Use of biometrics makes sure that an individual's information does not already exist in the hospital database. Biometrics can also deter fraud, because individuals who know that such a system is in place, it is less likely for anyone to try and register more than once.

Accountability

With HIPAA regulations looming over their heads, health administrators must be able to verify who has accessed specific files, at any given time, on a specific computer. Biometrics, combined with a computer operating system, provides administrators with more pronounced auditing and reporting capabilities. To understand how a biometric system works, it is important to know that a distinction exists between verification and identification. Verification tries to answer the question: "Am I who I claim to be?" An individual presents a user name, ID number, and then their biometric information. The system searches a database and determines whether the username and biometric information match the same information stored in the database. If a match is found, the user has been authenticated. Authentication is referred to as 1:1 (one-to-one) matching. Identification attempts to answer the question: Who am I? With the identification process, a user does not provide an identity, just their biometric information only. The system then compares this information with biometrics stored in the database. This is called 1: N (one-to-many) matching. It is obvious that one-to-many matching can be more time intensive and computational processing intensive.

The biometric process

The biometric process begins with enrollment. Depending on the type of biometric being used such as physiological or behavioral data, the details are acquired and then stored in the system as a template. One of the misconceptions regarding biometrics is that the system stores all the information, whether it is a fingerprint or scan of an individual's face. In reality, depending on

the system and the type of algorithms used, certain key features are extracted during enrollment and used to create a template. Each biometric vendor has its own enrollment algorithms, and some are better than others. A template can be stored locally on a PC or a network server.

To verify or identify a person, an individual must present his or her biometric information to the system. A template is created and then compared to the biometric stored within the system. The act of comparing a presentation template is matched with an enrollment template called 'matching'. When a presentation template is matched with an enrollment template, a score is generated. The score is generated based on the degree of similarity between comparisons of the two templates. A threshold number is set by the system administrator that establishes the degree of correlation necessary for a comparison between an enrollment template and a presentation template to be considered 'a match'. Depending on the level of security desired, the threshold can be set very high or very low. To understand the impact that a threshold can have on a system, it is important to understand the concepts of the 'false match rate', 'false non-match rate', and 'failure to enroll rate'. 'False match rate' is the probability that a user's template will be incorrectly judged to be a match for a different user's template.

Basically, this means that an imposter can succeed in logging onto the system, if the biometric information is similar to an individual already in the system. This is possible when the threshold is set very low. Changes in user's biometric data can occur. A person may get a cut or scratch on a finger. In facial recognition, a changed in hair style or glasses can affect non match rate. Therefore, no two presentation templates are the same. By raising the threshold, the system will require that presentation templates contain more biometric features than a lower threshold setting.

Drawbacks of biometrics in healthcare

Problems with finger-scan appear to be that not all user populations can be enrolled in the system, such as the elderly and individuals who do a lot of manual labour. Another drawback to finger scan is that the device used to collect presentation data can malfunction with wear and tear. This necessitates constant upkeep and replacement.

Drawbacks to the system include its difficulty in use. During enrollment and presentation, individuals must remain perfectly still, or the system will not be able to scan the iris. Therefore, causing non-matching and failure to enroll anomalies. Finally, users are sensitive to any device that shines a light into their eyes.

Integration of all services information together for better patient care management

A major problem with Healthcare Organisations (HCOs) is that many of the major systems that allow the organisation to operate are tied to disparate legacy information systems. For example, radiology may be running on a VAX, while accounting is using COBOL. Human resources and the medical records department (MRD) are still using paper to track employee and patient access. The MRD is working to adopt a new coding software program that may or may not work with proposed CPOE system being installed. From this brief description, it is easy to see that

many HCOs do not provide their administrators, physicians, and even their patients with the same seamless access that an integrated interoperable system could offer.

Business intelligence

It is necessary to provide the system with the answers to the patient's queries such as the type and number of operations a physician performs annually. This information can be made available to patients to help allay their fears and to assure them that they are in good hands.

The goal of Customer Relationship Management (CRM) is to tie the disparate system that operates within an HCO and to provide customers with greater access to information through a set of touch points. Again, these touch points can be traditional, such as telephones, television, fax, radio and prints. They could also be non-traditional and make use of new wireless technologies such as hand - sets, PDAs, and laptops. Furthermore, through the use of CRM, the HCOs can develop Web portals that allow patients to have the proper security clearance access to their medical records, laboratory results, and information about their physicians, such as the type of services, they provide and their educational background.

Potential and current applications

There are numerous healthcare applications which have or will benefit from the implementation of biometrics. These include, but not limited to Methadone clinics, Neonatal Intensive Care Units, Newborn nurseries, general and specialty care areas, admitting, pharmacy (electronic prescription), staff, time attendance, medical record management and PACS system etc.

Bioterrorism

Today's health systems must be fully prepared to support effective and efficient response to all hazards, even those with overwhelming casualties. The biometric security system can bring together the public health and public safety systems in the very near future. The threat of bioterrorist attack has grown very real since the "anthrax letters" of October 2001 in the Iraq war.

Biometrics, besides serving many purposes, could be very helpful in two other important ways. Firstly, the biometric-identification of terrorists can be distributed electronically to all potential risk areas within and outside the nation for preventive purpose. Secondly, it can help in detecting the disease while the number of seriously ill individuals provides a short interval to initiate aggressive treatment and prophylaxis measures that, if effective, would substantially reduce the mortality, morbidity and resource requirements following an attack. The suspected patients could be isolated to avoid further spread of contagious diseases.

The need to detect a potential bioterrorist attack has led to the introduction of numerous "bio-surveillance" systems. The primary focus of these systems is to detect the onset of nonspecific disease prodrome symptoms as early as possible before the patients present with classic disease syndromes or die of disease.

Public health surveillance

The new trend is driven by the need for early detection of surreptitious biological attacks. The trend is likely to accelerate because evidence is accumulating and these new approaches are successful. They can detect outbreaks earlier than existing methods and even identify outbreaks that have previously gone unnoticed. This trend has important implications for researchers and developers in clinical informatics because it is creating new design requirements for clinical information system.

The infectious disease threats

There are scores of infectious diseases which are of interest to public health and they are discussed and enumerated in both reportable diseases lists and threat lists. Past research suggests that outbreaks of such diseases fall into two key patterns that have very different implications for Information Technology, which we label as "Anthrax and Smallpox".

Early warning system

Public health surveillance systems have been defined as networks of people and activities that may function at a range of levels from local to international. In summary, current research is beginning to identify functional requirements for public health surveillance system that have implications for clinical information systems. Barriers to integration of clinical systems into public health include legal, administrative, and technical barriers. At present, health systems typically provide detailed information to public health only about patients with notifiable diseases, although public health has a legal basis to access any data needed for public health purposes.

Cost

In the case of biometrics, the high cost of the basic hardware has kept the technology from being a viable solution. Nine years ago, a fingerprint scanner was a bulky piece of hardware that cost around USD700. In 2006, they were available for less than USD100 and are smaller than a smart card. Intense competition has led to inevitable cost cutting.

Conclusion

There is a need to deploy two-factor authentication to properly secure protected health information. Deploy the right biometric device, in the right location, for the right group of users. The biometric plays a very important role in not only in maintaining privacy and security of healthcare management system but is of tremendous value in bioterrorism and public health activities in notifying infectious diseases and controlling mortality and morbidity rates by linking with curative hospitals.

References

1. Ball et al Healthcare Information Management Systems, Cases, Strategies, and Solutions Third Edition. (PP 02-103, 427-431,504-528)

2. Burrington, Jill et al. The Best of IN Confidence, (PP 175-189)

3. Carter, Jerome H., Electronic Medical Records (PP 13, 45)

4. Gates, Mary Ann, Biometrics-and the Passwords, "For the Record" Vol. 19, No.l16 P.14, August 6, 2007

5. Martin, Zack, "New Application for Biometrics" Health Data Management Magazine, December 1, 2007.

6. "Solving the Weakest Link in Healthcare Security: Passwords." DigitaPersona, February 2002.

7. Wager et al "Managing Healthcare Information Systems" (P271)