A Discussion of Security Requirements and Issues in Healthcare Information Systems

Rehab AlNemr
Hasso Plattner Institute
Potsdam University
Germany
rehab.alnemr@hpi.uni-potsdam.de

Prof. Dr. Christoph Meinel
Hasso Plattner Institute
Potsdam University
Germany
christoph.meinel@hpi.uni-potsdam.de

Abstract— The ongoing debate of using information technology to enhance the healthcare sector comes from the security vulnerabilities in current health information systems. In this paper we discuss the role of different security technologies in e-healthcare, the issues arise from applying security measures, and then state the requirements that should be taken into account to construct secure healthcare systems, and define some of the components to be implemented in these systems.

Keywords- Healthcare, Policies, Security, Trust

I. INTRODUCTION

E-health systems are information systems that deal with, store, process and analyze patient information. System participants are: medical organizations (hospitals, clinics, and pharmaceutical organizations) and healthcare professionals (doctors, physicians, nurses, pharmacists, etc.) who provide the healthcare services, insurance organizations who do the financing and patients who look for adequate treatment.

An Electronic Health Record (EHR) is developed to be a private lifetime record of an individual's key health history and care. It is of major value, providing a longitudinal view of clinical information. The EHR is patient-based, hence it contains valuable *information about the patient* like: ID and the demographic details like: name, national security number, date of birth, etc., *administrative information* like: current location, date of admission, dates of hospital visits, etc., and *clinical information* like: procedure codes, diagnoses, drug dosage, test results, etc. The record is available electronically to authorized healthcare providers and the individual anywhere and anytime in support of care. By time, the e-health systems became a large, heterogeneous network of systems with different security requirements, guarantees, and access policies. The collection, storage and communication of a large variety of personal patient data, however, present a major dilemma. How can we provide the data required by the new forms of healthcare delivery and at the same time protect the personal privacy of patients? And if we have strict policies for information disclosure, how can we be sure that disclosing only part of patient related information will not affect the physician decision of his treatment?

The public concern has been raised by disclosures of significant violations of confidential medical information. In Indianapolis, the medical records of patients of a psychiatrist, who treated sexual problems, were inexplicably posted on a web site accessible to the public. These records contained identifiable information such as names, addresses, and telephone numbers. Breaches of confidentiality have also occurred in major medical plans. A major Health Maintenance Organization (HMO), the Harvard Community Health Plan, until recently had maintained medical records containing detailed notes from psychotherapy sessions that were accessible to all clinical employees of the plan . At the University of Michigan Health System, patient records could be accessed by anyone through a publicly available search engine until this security breach was discovered [1].

Another security concern is *record contamination*. If the record was tampered with and the person is admitted to an emergency room, contaminated electronic medical records could quickly kill the patient, and nobody would know why. Moreover, imagine the value of having both the social security number of a person along with his dental record. Organized crime will be thrilled to have such information that identifies a person with no doubt.

Thus protecting privacy and confidentiality of individual health information is a critical issue. Privacy is not only sought by patients but also by medical practitioners: notably, many doctors strongly oppose solutions that would give central parties (such as health insurance organizations) the real-time power to monitor all their actions. Studies confirm that the most frequent breaches of patient information confidentiality do not come from unauthorized outsiders, but from uncontrolled secondary usage, accidental disclosures, curiosity, and subordination by insiders.

There is a misconception that such problems can be controlled by legalization and public regulations. This is a nonsufficient solution if at the electronic data flow level everything would be instantaneously traceable and linkable; for instance, how can organizations limit the collection of personal information if the infrastructure technology they use does not make it possible for them to do so? However that does not cancel out the important role of the legal rules in protecting medical information.

Such a debate is critical in order to ensure that the public policy and legislation will promote the use of IT that enhances healthcare rather than retard innovation in this field. Pursuing security means ensuring data confidentiality, authenticity, integrity, availability, accountability, anonymity, and access control.

Thus, security mechanisms that are necessary to be implemented in these e-healthcare systems are: strong user authentication procedure, digital signature technology, confidentiality protection of data in the system on the application, transport and network layers, privacy protection of the patient personal data, strong protection of the central healthcare database based on multiple firewall architecture, and PKI systems, which issue X.509 digital certificates for all users of the system (healthcare professionals and patients) - digital identities (IDs) for the users [2]. And since most e-health systems now are moving towards web portals, the XML standard formats are often used in these portals and accordingly the XML security plays an important role in these systems. Several tools have been developed to improve the security of XML files, which basically fall into two groups. One that improves the XML document itself by using encryption and digital signatures within the document and the other provides this functionality outside the XML document [3].

In this paper we are discussing the security services that e-health systems are trying to acquire, the related security technologies that are currently used, security solutions that must take into account data moving between different domains. Then we state the general requirements of a secure healthcare system and some of the system components that the system should have to achieve these requirements.

II. RECOMMENDATIONS OF PUBLIC E-HEALTH COMMUNITIES

Ensuring a high and consistent level of information security for EHRs, both within individual healthcare organizations and throughout the entire healthcare delivery system, requires organizations entrusted with healthcare information to establish formal information security programs [4].

The use of web portals offers astounding opportunities to share information between healthcare professionals and to reduce the costly paper trail. However organizations must create secure architecture to protect the privacy of patient records since main security requirements in healthcare, as well as in emerging mobile healthcare systems, include privacy and integrity of information related to patients [2].

The Cyber Security Industry Alliance (CSIA) has recommended ten steps in order to help foster development of a more secure healthcare information infrastructure. These steps include: deployment of strong authentication and authorization control methods using secure ID tokens, encrypting data that reside on storage devices using strong and standardized technologies to ensure confidentiality and privacy, proper disposition of retired information and equipments, conducting frequent system audits, using digital signature and secure date-time stamps to ensure data integrity and authenticity and using private data backbone through the use of private data network [5].

The Health Insurance Portability and Accountability Act (HIPAA) and the European Union Commission's Directive on Data Protection have stated a set of privacy and security regulations. They federally mandated regulatory standards are designed to limit the risks of loss due to breaches of privacy and security and, thereby, help create a safer environment for investments in advanced health information technology.

The e-DiaMoND project carried by a group of British scientists has summarized some of the generic security issues faced by e-Health projects. More or less they are the same security aspects and concerns described by the CSIA [6].

These are only a small set of many organizations and projects who believe that they can contribute to the development of a common framework to guide the protection of personal health information like: H*i*mss, NCQA, and JCAHO [4], [7], [8].

III. THE PRIVACY VS. POPULATION SAFETY DILEMMA

Early detection of biological events, electronic reporting of laboratory test results, efficient exchange of case reports across jurisdictions, and timely alerting of health threats are critical components of effective health protection. The IT security community will take part in the process of determining the security measures needed to maintain the balance between personal privacy and population safety.

An important activity in disease prevention, detection, characterization, and eradication is public health surveillance, the ongoing systematic collection, analysis, and interpretation of health data for the purposes of improving the health and safety of a population. Data are systematically collected and analyzed to determine what actions might need to be taken to prevent or control a disease or condition. Public health authorities like Center of Disease Controls (CDC) and the European Centre of Disease Prevention and Control (ECDC) generally rely on healthcare providers, laboratories, veterinarians, and others to report cases of reportable diseases and conditions when they are detected. Less commonly, health departments may contact or visit laboratories, hospitals, and providers to stimulate reporting of specific diseases and conditions. Nevertheless Laws and regulations do not force the states and private practice to report cases to the CDC or ECDC. Security countermeasures should be considered in order to protect public health while respecting and preserving personal privacy. The critical question is: What is the minimum information public health officials need to know to effectively protect the health of their constituency?

When security measures reduce the sensitivity of a syndromic surveillance system or impede a response to an outbreak or bioterrorist attack, they can contribute to health risk. On the other hand, disease surveillance systems and outbreak response systems can possess security vulnerabilities that increase risk to personal privacy. For example, a syndromic surveillance system that collects all data elements

within an electronic health record, rather than a restricted, de-identified data set, increases risk to privacy [9].

IV. CONFIDENTIALITY AND PRIVACY PROTECTION

Healthcare records contain a large amount of sensitive and personal data. That information may range from demographics including age, sex, race, and occupation, to financial information such as diagnoses of AIDS, mental illness, alcohol abuse, or treatment. Regardless of the nature of information dissemination or storage, people have the right to protect their confidential information from unnecessary public disclosures. This should be done by using digital envelope technology based on symmetrical and asymmetrical cryptographic techniques and PKCS#7 file format. This technology is based on digital certificate, symmetrical algorithms for encryption of data and asymmetrical algorithms for protection of symmetric key which is sent together with encrypted data [2].

Furthermore, to allow secure sharing of health records between different healthcare providers, Right Management Techniques facilitating a data-centric protection model can be employed: medical data are cryptographically protected and allowed to be outsourced or even freely float on the network. In this technique, data are protected at the end points of the communication rather than relying on different networks to provide confidentiality, integrity and authenticity [3].

Rights Management Technologies or Enterprise Rights management (ERM) are increasingly used to protect business documents in order to counter the threat of unauthorized access and distribution of corporate data. The system enables protection of sensitive information from unauthorized use by allowing the data owner to define usage rights and conditions. The data owner protects the data by encrypting it within a protected data container. In the domain of healthcare, some pilots have already been set up to control distribution and usage of Electronic health Records with existing ERM architectures. The aim is that healthcare providers can securely share confidential patient files with business associates and patients in accordance with the HIPAA using the protection of the underlying ERM technology. The ERM framework enforces policies governing access to sensitive information, but also ensures protection if information is distributed beyond organization boundaries [3].

V. AUTHENTICATION AND INTEGRITY USING DIGITAL IDENTITIES AND HEALTH CARDS

HIPAA refers to *data integrity* as to the condition that protected health information (PHI) has not been altered or destroyed in an unauthorized manner. This includes prevention of authorized individuals making unauthorized changes to the medical information as well as unauthorized people altering this information [3]. Authentication process can be realized by using:

- Username and dynamic password obtained by appropriate hardware token, or by
- Username/password and PKI smart card and a challenge response procedure based on PKI X.509 and asymmetrical cryptographic techniques.

Either way the user (who can be any of the system participants) needs a digital identity to be authenticated to the local domain or to other domains by using a smart card that has all user related information and digital certificate.

In the last years, many of the EU countries set up programmes for electronic health cards, which are also designed to support processes around healthcare. Since this introduction consolidates the telemedicine processes also from a legal point of view, governments decide to put an integrated identity management in place [10].

VI. ACCESS CONTROL AND AUTHORIZATION

Access control and authorization mechanisms are essential in protecting sensitive patient information. These mechanisms should provide for simultaneous access to different patient data, for example, health history, patient-case data, administrative data and the like. [11]

The case is different if the user is attempting to access information within the local boundaries of a medical organization or from other domains.

A. In one local security domain

Up to the present days, most e-healthcare systems are islands where all the data resides within one administrative domain. This domain is not or hardly accessible from the outside, and the set of users operating on the data is reasonably small and static. In these systems the access control process matches the data, the accessing party, and the data policy to determine whether or not access to the data should be granted. To this end the user first needs to be authenticated, i.e., the user identity is established. Secondly the system evaluates the data policy to determine if access should be granted. The special challenges in a medical environment are that access to the data is very context dependent, and roles of medical personnel may change quickly- an expert on a certain disease can rapidly turn from visitor to acting doctor. A doctor also should never be blocked from data access in an emergency [3].

B. In multiple security domains

As the healthcare marketplace becomes more open and competitive, data management solutions must take into account that data move between different domains. Applications will need to select and interact with multiple providers and multiple security domains, trust management systems will be required to establish high levels of trust [3] [12].

1) Security Policies

Consider a healthcare system where patient's records are kept in a large information system that is connected to hospitals nation wide. The agents, or participants, of this system are, but not limited to: Doctors, Nurses, Specialists and paramedics. When a patient's record is to be requested by one of the system agents, polices are checked to grant access to the requester. *Authorization and Access control* policies in this

environment will discover the services and information of interest from the infrastructure and other devices in the vicinity, negotiate for access, control information exchange and monitor for suspicious events to be reported to the community. *Privacy policies* will keep certain information from being disclosed, the doctor can choose not to disclose certain information concerning a patient to anyone, e.g.: Drug Dependency, data on fertility and abortions, emotional problems and psychiatric treatment [13].

2) Trust Negotiation

Traditional access-control methods describe access conditions in terms that only apply to parties within the local security domain. Within a security domain, communicating parties share a pre-existing relationship in which access criteria and permission levels are already defined prior to a transaction taking place. For example, protecting sensitive data with password and/or biometric schemes are popular security techniques but require foreknowledge of the communicating parties (e.g., the access-granting system must compare the requestor's password with a pre-established password list). Current Public Key Infrastructure (PKI) systems store the participants' certificates in a centralized repository and assume prior knowledge of the subject identity listed in each certificate. A significant problem arises when no prior relationship exists between an access-granting service and a party requesting EHR data. For example, consider the common situation of healthcare provider *A* requesting a patient's EHR from hospital *B,* where *B* cannot authenticate *A's* request because they are strangers (i.e. they have no foreknowledge or preexisting relationship) [14].

Trust negotiation is the process of establishing trust among interacting parties in distributed and decentralized systems. It is the most appropriate process when an individual outside a local security domain wants to access sensitive data and services. For example: if a patient needs to consult a physician while staying abroad, or even out of town. In this case the physician will request access to the patient's medical record. The trust negotiation process is triggered: receiving the policy that entitles the physician to access these records and accordingly sending his credentials, verifying the signed credentials, and initiating an encrypted session to transfer patient record.

VII. REQUIREMENTS FOR A SECURE HEALTHCARE SYSTEM

Given the above overview of security measures, we can summarize the main requirements or guidelines of a secure healthcare system as to provide an information system that:

1. Complies with the legalization laws that govern both public and individual privacy without hindering the information system or the diagnosis and treatment process.
2. Deals with the public *safety-versus-privacy* dilemma efficiently and quickly. It should be able to recognize disease outbreak patterns, bio-attacks and override the security policies if needed. Mass health surveillance must be operated under restricted conditions and policy overriding should be tagged through auditing system for further investigation. The auditing systems should also track information disclosure to determine whether they compiled with laws or not.
3. Processes and analyzes data efficiently. Recording where data are kept and stored, where they are sent, who processes them and who access or modify them. This will help in policy composition and in categorizing security levels. Thus the system will be capable of retrieving the requested data on time for authorized personal without revealing unnecessary information.
4. Preserves patient privacy. This includes: patient identity, personal information, medical records, and treatment process. Nevertheless the protection must be implemented without constraining proper use and dissemination of health data or inhibit scientific discovery.
5. Applies access control and authorization methods through all the phases of treatment even if the requested data are outdated or seemed irrelevant.
6. Defines extensible trust hierarchies and levels, and implements subjective trust models that depend on dynamic trust intervals rather than specific values (i.e. derived from reputation-based trust models).
7. Enforcing privacy and authorization policies in both database level and application level. In database level all queries are to be executed on the data source so that the application only retrieves results that are compliant with both system's and patient's disclosure policies. For example if a medical researcher wrote a query requesting information about all patients who recently suffered a certain disease, the system filters the information and returns only the data that can be revealed for each patient.
8. Verifies data authenticity and integrity.
9. Enables information retrieval independent of patient location –decentralized information system. The information should be available if the patient is treated outside his normal domain (i.e. another city or country). The information is transferred and processed securely between multiple security domains through trust negotiation methods.
10. Offers flexible yet secure information retrieval in case of emergencies. An emergency here is identified as a situation where the patient is either admitted to an ER or about to have a major surgery. The categorization of a major surgery is defined by the medical engine of the system components.
11. Presents anonymous consultation possibility. In some cases it is suitable to remain pseudonymous. Often, if some personal identities are disclosed, it might make the patient disadvantaged or threaten,

e.g. patient who possesses fatal disease identifier, such as Acquired immunodeficiency syndrome (AIDS) or a severe mental disease [15]. Also patients might want to anonymously consult expert systems about mental healthcare, psychiatric and/or psychological advice, etc.

12. Enables user-policy control through user friendly interface, where the patient has the right to state who can access his information and what to access. Nevertheless, given the non-medical background of most of the patients, there should be reasoning against some user policies i.e. hiding a disease that will affect the diagnosis and treatment of other disease. User control is not limited to policies but also to decisions such as subscribing to a medical service, whether the user's medical insurance company should be included in each service provisioning and workflow and so on.
13. Identifies policies conflicts and enables fast conflict resolution. The conflict can be between system policies or between system policies and user policies. For example if the user chooses not to reveal his address to any third party (rather than the hospital) and one of the system policies is to release information to relevant government agencies or according to a court order, then the user should be notified of the conflict.
14. Allows *Policy-transition* capability. That is, when a patient agrees to provide personal data to a healthcare organization, he/she is entering into an agreement regarding the handling of his/her data. If data transfer is allowed, the patient should be assured that the same disclosure rules will apply to the data after transfer.
15. Enables equal security levels for mobile healthcare systems that include handheld computing platforms and wireless communication technologies. The challenge comes from both the broadcast nature of wireless transmission as well as the resource limitations (including bandwidth, processing capability, battery life, and unreliable connections) of many devices that populate wireless networks. Trust management techniques will be an essential part of both the general and mobile security model.

VIII. SYSTEM COMPONENTS

In order to fulfill the above requirements, a general prototype of the system components should be exploited. These system components should be dynamic and interoperable enough to be used with different healthcare information systems.

Healthcare portal and Health record database: The web application acts as an interface for systems that deal with, store, process, and analyze patient information. Patient information is stored in a large database that is connected to the portal.

Mobile Interface: The long vision is that healthcare systems are extended to monitor patients with body sensors wirelessly linked to a mobile phone that interacts with remote healthcare services and staff. The mobile phone will act as a gateway that will be able to communicate with the body sensors and with remote services and medical staff using a mobile voice/video/data standard like 3G [12]. Moreover the doctors will have handheld devices that provide them with patient related information almost instantly.

Policies and Negotiation engine: States terms of who can do what under which circumstances. It contains both organization policy composition as well as user-control policy creation processes. In order to establish trust between system entities, credentials are disclosed gradually by requesting, in an iterative process, to fulfill the system policies. This engine is responsible for stating the relative costs and benefits of secured interaction, unsecured interaction or no interaction at all.

Auditing engine and interface: tracks the identities of users who have accessed any cell in the database, the date and time of access, the purpose of the access, the recipient of the information and the exact information disclosed.

Medical Categorization engine: that is edited by medical specialists and the reasoning engine. It can be viewed as a large processed knowledge base. Four building blocks are specified

- *Disease-outbreak* block that defines the patterns which recognize public health threats and epidemic diseases. It is part of the public health surveillance system and it can be associated with the appropriate contingency plan. When these patterns occur, policies can be overridden for the sake of the public safety.
- *Disease categorization* block that clusters diseases according to their seriousness (e.g.: Life threatening, contagious… etc). The category of the disease is used as a factor in the decision making process (what to reveal , whom to reveal to, what policies to be changed or overridden)
- *Roles categorization* of the medical participants block. Beside the direct role of system participants (general practitioners, specialists, nurses, hospitals…..etc), the participants are dynamically categorized into clusters of importance according to the disease, position, and current situations.
- *Context categorization* block. A complex plot that has an important role in and majorly edited by the reasoning engine. The engine gathers information then clusters the *situations* in terms of context that are used as factor in decision making. *Situations* can be bioterrorist attacks, disease outbreak that is inferred by the reasoning engine and according to patterns defined in the dieses outbreak block. Or *Situations* like dying patient, patient who is affected physiologically by an

external factor, or patient having major surgeries. The semantic meaning of the term *situation* can be entered by a medical specialist.

Reasoning engine: is the brain of the healthcare information systems which is used in the decision making process. The engine capabilities are, but not limited to:

- Responsible for information extraction and analysis from all the engines, as well as defining data interaction between them.
- Carries the conflict recognition and resolution processes between the policies and suggest proper solution.
- Feeds the policy composition process. Policies updating or overriding are carried out as a result of a conflict resolution process, user added policies, change of organization policies or public laws. Also it is responsible for updating the trust negotiation process given the current factors.
- States the amount of risks and costs taken by blocking some information or by denying access at all. i.e.: requesting the medical information for a patient who is admitted to the ER and finds that the information associated to his allergic reactions unavailable.
- Analyzes the patterns connected to a disease outbreak and delivers a decision of what information to be revealed accordingly. Also delivers proper decisions in case of patient emergencies.

IX. CONCLUSION

Managing records of patient care has become an increasingly complex issue with the widespread use of advanced technologies. The vast amount of information for every routine care must be securely processed over different data bases. Data privacy is a growing concern among healthcare sector, which are entrusted with the responsibility of managing patient information. In this paper we have outlined the security mechanisms that are essential to implement a secure healthcare system.

As the e-health systems are becoming more pervasive and the need to share information between different domains is becoming more important, the use of policies and trust management techniques is a must rather than an option. Trust management is used to help an entity in authentication when there is no prior knowledge between the requester and the receiver. It is also critical to use it in mobile pervasive systems.

Auditing systems are required to track past disclosures of information to determine whether they abide by legalization laws. Hippocratic Database (HDB) Compliance auditing system enables organizations to investigate past disclosures without the performance and overhead burdens. This is done by logging relevant database queries and updates and allows auditors to track the identities of users who have accessed any cell in the database, the date and time of access, the purpose of the access, the recipient of the information and the exact information disclosed [16].

We have presented the requirements that should be realized by the implemented system components in order to have a secure healthcare system. Future work will be providing detailed outlines of each system component and have a thorough investigation of how to ensure the delivery of each of the mentioned requirements.

Finally, in the light of advanced technologies and the deployment of artificial intelligence, further security concerns should be examined. It is not unfeasible to have an engine with reasoning capability to deduce patient information through obtaining several pieces of seemingly unrelated information.

REFERENCES

[1] James G. Anderson**,** "Security of the distributed electronic patient record: a case-based approach to identifying policy issues", International Journal of Medical Informatics, Volume 60, Issue 2, 1 November 2000, Pages 111-118.

[2] Milan Marković, " On secure e-Health systems", Book Chapter: Privacy in Statistical Database, Volume 4302/2006, pages 360-374

[3] Milan Marković, Stefan Katzenbeisser and Klaus Kursawe, "Rights Management Technologies: A good choice for securing Electronic Health record?", ISEE/Secure proceeding, Poland 2007.

[4] The Healthcare Information and Management Systems Society: http://www.himss.org/ASP/index.asp

[5] Cyber Security Industry Alliance Technical report: Ten Steps for Securing Electronic Health Care Systems, April 2005

[6] Mark Slaymaker, Eugenia Politou, David Power, and Andrew Simpson, "e-Health security issues: the e-DiaMoND perspective", The eDiamond project, University of Oxfrod

[7] The National Committee for Quality Assurance: http://web.ncqa.org/

[8] The Joint Commission: http://www.jointcommission.org/

[9] Dixie Baker, "Maintaining the delicate balance between personal privacy and population safety", Computer Security Applications Conference, December 2006, pages 3 - 22

[10] Christoph Meinel, Matthias Quasthoff, "Identity Management in Telemedicine", In Proceeding Winter course of the CATAI, La Laguna, Tenerife, Spain, 2006.

[11] Song Han, Geoff Skinner, Vidyasagar Potdar and Elizabeth Chang, "A framework of authentication and authorization for e-Health services", Proceedings of the 3rd ACM workshop on secure web services 2006, Pages: 105 – 106.

[12] Changyu Dong and Naranker Dulay, "Privacy preserving trust negotiation for pervasive Healthcare", in IEEE Pervasive Health Conference and Workshop, December 2006, pages 1-9.

[13] Lalana Kagal, Tim Finin, Anupam Joshi and Sol Greenspan, "Security and privacy challenges in open and dynamic environment", IEEE Computer society, Vol. 39, No. 6, June 2006.

[14] David K. Vawdrey, Tore L. Sundelin, Kent E. Seamons, and Charles D. Knutson "Trust negotiation for authentication and authorization in Healthcare Information Systems", Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society,Volume 2, Issue 17-21 September 2003

[15] Jieun Song and Myungae Chung,"An approach to realization and security provision of intelligent U-Healthcare Service", Electronics and Telecommunication Research Institute, Daejeon, KOREA.

[16] Rakesh Agrawal Roberto Bayardo Christos Faloutsos Jerry Kiernan Ralf Rantzau Ramakrishnan Srikant. "Auditing compliance with a Hippocratic database", Proceeding of the 30th International Conference on Very large Databases, Toronto, Canada, August 2004.