Security Issues and Aspects in Healthcare Pervasive Systems

Christoph Meinel, Rehab AlNemr
Hasso-Plattner Institute, Potsdam University, Germany

Abstract— **Electronic Healthcare is a rapidly growing area that has attracted major attention due to its critical impact on the quality of life. Security and privacy issues arise from the dramatic increase in the role that IT plays in the delivery of healthcare. In this paper we discuss the role of different security technologies in e-healthcare and mobile e-healthcare systems and the need to select and interact with multiple providers and multiple security domains. As e-health systems are becoming more pervasive, trust management systems will be required to establish high levels of trust.**

***Index Terms*—Security, healthcare, Trust, Privacy**

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? But 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. In this paper we are discussing the security services that e-health systems are trying to obtain, the related security technologies that can be used, security solutions that must take into account data that moves between different domains, and the future security concerns of Mobile healthcare.

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 [2].

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 [3].

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 resides 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 [4].

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 the generic security issues faced by e-Health projects. More or less they are the same security aspects and concerns described by the CSIA [5].

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 [2], [6], [7].

III. General security Services and mechanisms

Let us take a step back and perceive what we are seeking to achieve in general. We are trying to ensure that security services are implemented within the structure of any system. These services enhance the security of the data processing and the information transfers of an organization. The services counters security attacks and makes use of one or more security mechanisms (cryptographic techniques) to provide the services. One usual classification of security services is the following [8]:

A. Confidentiality

Confidentiality ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties. Most medical data is highly personal and sensitive. Accordingly, it is to be protected from unauthorized disclosure during transmission as well as during storage [9].

B. Integrity

Integrity ensures that only authorized parties are able to modify computer system assets and transmitted information. Authenticity and Integrity requires that an attacker will not be able to substitute a false ciphertext C` for a ciphertext C without detection. Since medical data is a critical data, and even sometimes life threatening data, integrity of medical data transferred either via wired or wireless networks should be ensured.

C. Authenticity

Authentication ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false. Strong user authentication both for doctors and other medical employees, as well as for patients is needed.

D. Access Control

Access Control requires that access to information resources may be controlled by or for the target system. Access decisions can be based on the roles that individual users have as part of an organization (doctors, nurses, etc.) , upon presentation of a document of identity or based on authorization tickets.

E. Availability

The availability of the data when it is required is of an essential importance to the health sector. Imagine requesting the medical information for a patient who is admitted to the ER and find that the information associated to his allergic reactions unavailable.

F. Non-repudiation

Non-repudiation requires that neither the sender nor the receiver of a message be able to deny the transmission.

G. Anonymity

Occasionally it is necessary to reveal identifying personal data, e.g. when being asked by a hospital to pay for the treatment service or to identify patient exactly for high reliable treatment. However, in other cases it is suitable to remain pseudonymous or anonymous. 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, should be taken with 'The Scarlet Letter' unknowingly [10].

Also patients might want to anonymously consult expert systems about mental healthcare, psychiatric and/or psychological advice, etc.

These services are to be ensured by means of security mechanisms. Encryption techniques are the main key to ensure the deployment of these services. In general there are two categories of encryption algorithms: Symmetric and

Asymmetric algorithms. The difference is that symmetric algorithms use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key) and the encryption process is faster, whereas asymmetric algorithms use a different key for encryption and decryption (the decryption key cannot be derived from the encryption key) and it is much slower. Therefore, symmetric encryption is used to encrypt large amount of data where asymmetric encryption is used only to ensure data authenticity and integrity by means of *digital signatures*. Digital signatures are the counterparts of personal signatures that are used in everyday life as authentication mechanisms. By encrypting a small amount of data using the sender's private key and attaching it to the message, both the source and the integrity of the message are validated. Digital Certificates are used to ensure that the holder of the public key belongs to the person it claims to represent. Certification centers work as trusted third parties that states authoritatively to whom a public key belongs. A widespread format for digital certificates is the one according to the ITU-T X.509 standard. The X.509 standard furthermore defines how to verify the validity of certificates. Instead of requiring all certificates being signed by the same trusted third party, *public key infrastructures* (PKI) are established. A PKI specifies a root *certificate authority* (CA), which all participants need to trust. This root CA then certifies other CAs or possibly individuals and so on [8], [11].

IV. Security infrastructure in e-Healthcare systems

The use of multi-layered security infrastructure is suggested to be the solution to cope with possible attacks to e-healthcare systems. The benefit is to protect patient confidentiality from network-based violations, securely provide information to remote physicians, partners, and branch offices, and comply with government regulations on network security [3].

The Multi-layered security infrastructure consists of security mechanisms on three different ISO/OSI reference model layers:

- Application level security (end-to-end security) based on the strong user authentication, digital signature, confidentiality protection, digital certificates and hardware tokens (e.g. smart cards),
- Transport level security based on establishment of a cryptographic tunnel (symmetric cryptography) between network nodes and strong node authentication procedure,
- Network IP level security providing bulk security mechanisms on network level between network nodes – protection from the external network attacks.

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 [3].

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 [12].

V. Ensuring authentication and integrity using digital identities

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 [12]. 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.

VI. Digital Signatures using health cards

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 [13].

Three types of digital identity cards are introduced: *Health Insurance Cards* for patients, *Health Professional Cards* for medical practitioners and pharmacists and *Secure Module Cards* for medical practices and pharmacies to be used by their employees. Each holds the digital certificate of its holder and each digitally signs the corresponding data whenever used, thus ensuring the authenticity of the signature. The private key is generated on some of these cards and it never leaves the card. The signature made by e-Health PKI cards follows the EU Electronic Signature Legislation rules [13].

VII. 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 [3].

A. *Enterprise Rights Management*

In order 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 is cryptographically protected and allowed to be outsourced or even freely float on the network. In this technique, data is protected at the end points of the communication rather than relying on different networks to provide confidentiality, integrity and authenticity [12].

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 [12].

B. *Protection of the central Database*

Recently a joint research between IBM and Microsoft focused on protecting the database that contains the health records in each organization. Their research confirms that policies concerning the disclosure of electronic health records can be reliably and efficiently enforced and audited at the database level.

Their approach is called the *Hippocratic Database approach.* It is an integrated set of technologies that manages disclosure of electronic health records in compliance with data protection laws without impeding the legitimate flow of information. HDB's Active Enforcement component limits disclosure of personal health information at a fine-grained level in strict accordance with enterprise policies, legal regulations, and individual patient choices. Its Compliance Auditing component efficiently tracks past disclosures to verify compliance with these policies. Finally, its data mining, de-identification, and information sharing components enable organizations to derive maximum value from sensitive data without compromising privacy or security [14].

VIII. Authorization and Access Control

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. [15]

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 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 [12].

B. *In Multiple Security Domains*

As the healthcare marketplace becomes more open and competitive, data management solutions must take into account that data moves 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. [16], [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 [17].

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) [18].

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 will be triggered: receiving the policy that entitles the physician to access these records and accordingly send his credentials, verifying the signed credentials and initiate an encrypted session to transfer patient record.

IX. Mobile Healthcare

Healthcare systems are being 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. Obviously the e-Health mobile system will inherit the security concerns associated with the mobile pervasive systems. People will be able to decide and even negotiate which services they want. For example, a user will be able to subscribe to a medical monitoring service that can process the readings from the user's sensors forwarded via the user's mobile phone. If an emergency is detected the monitoring service could inform the user, the user's doctor and call an ambulance. The monitoring service will need access to the user's medical details that are relevant to the monitored condition as well as details of the hospital where the user may have had previous treatment for the condition. The monitoring service would then be able to liaise with the emergency services and the hospital to which the user will be taken for emergency treatment. Hospitals may need to interact with the user's doctor and possibly social services about caring for the user after treatment. In a small hospital, there may not be local expertise to evaluate medical information such as X-rays and ECG readings and so these need to be sent to a remote expert over the network. Perhaps the user's usual consultant is not available and a new one has to be chosen. In some contexts, the user's medical insurance company will need to be included in the service provisioning and workflow. The monitoring service may like to provide anonymous monitoring records of the user for medical research perhaps by offering a discounted price for the service

Issues of trust, privacy, security and context pervade this simple scenario. Should the user trust the monitoring service? Can the user verify the credentials of the monitoring service? Can the user ensure that only those parts of his medical record pertinent to the monitored condition are disclosed by the user's doctor/hospital to the monitoring service? Should the user allow his monitored data to be anonymous and passed on? Should the hospital trust the monitoring service? Should the hospital rely on the data and assessment from the monitoring service? Should the monitoring service trust the user and the readings from the user's sensors? The list is long. Even when the general workflow of service interactions is known, circumstances (context) will require decisions to be made dynamically. We would like to localize and automate these decisions as much as possible. In particular we would like the decision on whether a connection (secure on or not) should be established with a particular party to be based on local policies. We also want privacy preserving policies that can be used to control what information should be disclosed (including the credentials used) in the trust negotiation process. The other party will do likewise, leading to a degree of mutual trust [16].

Trust management is a more flexible means of establishing and evolving security and privacy in distributed, mobile and pervasive systems than the traditional centralized model because it does not require pre-knowledge of users and services or a common security infrastructure. Such an approach will be essential in pervasive healthcare where applications will need to support legal requirements for user privacy and data protection [16].

A. Trust Negotiation in Mobile healthcare systems

Healthcare information systems, that include handheld computing platforms and wireless communication technologies, manifest numerous security challenges beyond those in conventional health information systems. These difficulties arise 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. Unfortunately, many of the algorithms used in standard trust negotiation require computationally intensive cryptographic calculations and reliable access to the Internet that may not be possible for typical resource-limited mobile computing devices. Surrogate Trust Negotiation provides a flexible model that effectively leverages the combined capabilities of network proxies, software agents, and modern cryptographic systems. The highly sensitive and resource-intensive task of public key cryptography that is integral to credential-based systems is offloaded to *trust agents.* Trust agents are autonomous software modules on secure, offsite computers that act as "surrogates" for mobile devices, performing cryptographic operations and managing credentials, policies, and secret keys for use in trust negotiation. Thus, STN allows even computationally lightweight devices to effectively participate in data exchange scenarios using trust negotiation [18].

X. Between personal privacy and population safety

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.

Although it is not entirely within the scope of our paper to discuss the effect of personal privacy laws on the public safety, 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 Diesis 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 [19].

XI. 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.

Security mechanisms that are necessary to be implemented in the 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 digital identities (IDs) for the users.

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 used also in mobile and pervasive systems.

At the end of our paper, we refer to a critical issue of constructing privacy policies that keeps the balance between personal privacy and population safety. Selecting which potentially identifiable data elements to include in any data-collection scenario or data exchange is a risk management decision.

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 certain information. For example: blocking the medication information but providing some allergic and blood reaction information will enable the engine to infer patient diesis or any other personal 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] The Healthcare Information and Management Systems Society: http://www.himss.org/ASP/index.asp

[3] Milan Marković, “ On Secure e-Health Systems”, Book Chapter: *Privacy in Statistical Database*, Volume 4302/2006, pages 360-374

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

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

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

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

[8] William Stallings, Cryptography and Network Security, Second Edition, Prentice Hall, ISBN:0-13-6869017

[9] Gerrit Bleumer, “Security for Decentralized Health Information Systems” International Journal of Biomed. Comp. 139-145; Feb. 1994.

[10] Jieun Song and Myungae Chung,”An Approach to Realization and Security Provision of Intelligent U-Healthcare Service”, Electronics and Telecommunication Research Institute, Daejeon, KOREA.

[11] RSA Data Security Inc., “Public Key Cryptography standard”, Technical standards, 2004.

[12] Milan Marković, Stefan Katzenbeisser and Klaus Kursawe, “Rights Management Technologies: A Good Choice for Securing Electronic Health record?”, ISEE/Secure proceeding, Poland 2007.

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

[14] Rakesh Agrawal and Christopher Johnson, “Securing Electronic Health records without impeding the flow of information”, International Journal Medical Information 2007

[15] 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.

[16] Changyu Dong and Naranker Dulay, “Privacy Preserving Trust Negotiation for pervasive Healthcare”, in IEEE Pervasive Health Conference and Workshop, December 2006, pages 1-9.

[17] 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.

[18] 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

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