Tomasz HYLA, Jerzy PEJAŚ
WEST POMERANIAN UNIVERSITY OF TECHNOLOGY,
DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

A security architecture of an inter-jurisdiction EHR system

MSc Eng. Tomasz HYLA

PhD student of the Software Technology Department of the West Pomeranian University of Technology, Szczecin. He received M.Sc. degree in Computer Science and Engineering from the Szczecin University of Technology in 2007. His research interest includes IT security applied to electronic health records (EHRs).

e-mail: thyla@wi.zut.edu.pl

PhD Eng. Jerzy PEJAŚ

He received M.Sc. degree in Computer Science and Engineering from the Wrocław University of Technology and PhD degree in Control Systems from Gdansk University of Technology. Main subjects of interest: information and computer network security, methods of secure electronic signatures as well as new trends in applied cryptography. Employed as Associate Professor at the Faculty of Computer Science and Information Technology, West Pomeranian University of Technology, Szczecin.

e-mail: jpejas@wi.zut.edu.pl

Abstract

An Electronic Health Record (EHR) is a virtual container composed of healthcare related documentation linked to one patient. An EHR system manages and allow access to the EHR's. A few architectures of nationwide EHR systems were reviewed and classified by EHR documents' storage location. An inter-jurisdiction general model of an EHR system was created using this classification and international standards. The security of such complex system, which must process data from hundreds of millions people, is a major concern. Security requirements for such system together with and proposition of security subsystems, which are necessary to protect EHR system are presented.

Keywords: electronic health record (EHR), EHR system, security, registry, inter jurisdiction system.

Architektura bezpieczeństwa międzyjurysdykcyjnego systemu EHR

Streszczenie

Elektroniczny dokument zdrowotny (EHR) jest wirtualnym kontenerem złożonym z dokumentacji zdrowotnej powiązanej z jednym pacjentem. System EHR zarządza i umożliwia dostęp do elektronicznych dokumentów zdrowotnych. Rozwój systemów EHR jest priorytetem w państwach należących do Unii Europejskiej. W artykule przedstawiono i sklasyfikowano kilka architektur krajowych systemów EHR z punktu widzenia lokalizacji przechowywanych dokumentów EHR. Dokumenty wchodzące w skład EHR mogą być przechowywane w centralnych repozytoriach krajowego systemu EHR lub mogą znajdować się w repozytoriach lokalnych systemów instytucji ochrony zdrowia, a ich metadane umieszczone są w centralnym rejestrze. Każde z tych rozwiązań ma swoje wady i zalety. Następnie w oparciu o tę klasyfikację oraz normy międzynarodowe zaproponowano ogólny międzyjurysdykcyjny model systemu EHR. Model posiada budowę modułową i ukrywa swoją wewnętrzną strukturę przed użytkownikami. System międzyjurysdykcyjny może łączyć wiele państw o odrębnych przepisach prawnych, które ustalą sposoby wzajemnego dostępu do danych medycznych. Głównym wyzwaniem tak złożonego systemu, w którym muszą być przetwarzane dane setek milionów pacjentów jest jego bezpieczeństwo. Problemy bezpieczeństwa trywialne w małych lokalnych systemach są bardzo skomplikowane. W artykule zaprezentowano wymagania bezpieczeństwa nakładane na takie systemy znajdujące się w ISO TS 18308 wraz z propozycją podsystemów bezpieczeństwa, niezbędnymi do ochrony systemu EHR.

Słowa kluczowe: elektroniczny dokument zdrowotny (EHR), system EHR, bezpieczeństwo, rejestry, system międzyjurysdykcyjny.

1. Introduction

Nowadays, the development of nationwide healthcare systems is a priority of many countries around the world. In the European Union, due to the European Commission directives and plans for development of an information society, a pan-European EHR system is a long term goal. An EHR system manages and allow access to an EHR (Electronic Health Record).

An EHR is a virtual container composed of healthcare related documentation linked to one patient. Clinical documents, which are a part of an EHR, are spread among many different repositories and registries. The architecture of nationwide EHR systems, depending on a local policies and conditions, can be designed in a few different ways. The next step, is development of an international EHR system, e.g. future EU EHR system, which will connect all member countries. The security of such complex system, which must process data from hundreds of millions people, is a major concern. Also, international systems must have built in solutions for solving security problems related to different national legislations.

This paper presents security measures for a general model of an international EHR system. The section 2 presents architecture of a few chosen nationwide systems and a general model of an EHR system based on these systems and on international standards. Section 3 proposes security measures for such general system and section 4 contains summary and discussion.

2. Inter-jurisdiction EHR system architecture

2.1. National EHR systems

EHR systems are developed in many countries in the world, as they improve the quality of healthcare [1-4] and reduce costs. An adoption rate and functionality of EHR systems varies [5-8]. Different local conditions, policies and requirements result in different approaches to the design of EHR systems. However, architectures of these systems can be classified into a few basic categories according to clinical documents' storage location.

2.1.1. Canada

Canadian nationwide Electronic Health Record system is being developed by non-profit organization called Infoway [9]. By the 2010 50% of Canadians should have their EHR available and by the end of the 2016, 100% [10]. The pan-Canadian EHR system is divided into a lot of (even up to 40) regional infostructures. Single EHR infostructure consists of five general repositories of clinical information (Shared Health Record Repository, Laboratory Tests Results Repository, Drug Information Repository, Diagnostic Images Repository, Immunization Repository) [11] and consists of several registries (client registry, provider registry, user registry, location registry), which stores information about subjects of care, healthcare professionals and healthcare sites. There are also some auxiliary registries, e.g. repository of technology, database of message structures. In total, in the EHR infostructure may be up to 15 different repositories and registries. The internal system database structure is hidden from the users and system can be accessed only by HIAL (Health Information Access Layer). All clinical information stored in the system is indexed in an indexing registry; also there is an EHR locator service that has information about patients registered in other infostructures. After a clinical data is entered to the PoS (Point of Service) system (e.g. a hospital information system (HIS), a pharmacy system or a physician's office EMR system), the PoS system sends the message to HIAL. The HIAL parses the message, extracts all relevant information and inserts new records to appropriate repositories and registries.

2.1.2. United Kingdom and Estonia

Another approach to an EHR system structure is used in the United Kingdom in Estonia and in Germany. In the United Kingdom [12] one nationwide medical registry was created, which stores basic information about patients e.g. name, surname, blood type, allergies and performed surgeries. The registry is called a Summary Care Record (SCR) and enables access to basic healthcare data from every part of the country, e.g. in emergency situations. However, it was recognized that system, which stores more detailed clinical information is needed, and DCR (Detailed Care Records) registry system was introduced. The DCR system does not have a nationwide registry. Instead of that, the system is composed of regional DCR registries and composed of main registry which contains links to regional registries. Healthcare sites (e.g. hospitals, General Practitioners (GPs)) can still stores information in their local registries. The registries must conform to recognized standards and must enable communication and transfer of clinical data to registries in other healthcare sites.

The idea of Estonian EHR system is similar [13, 14]. Estonian central EHR database contains three types of clinical data patient’s basic information, link directory which contains links to other registries in local healthcare sites and centrally stored medical records. In Estonian EHR system is possible to connect existing local registries, similarly to the UK, it is only required that the local registry must have abilities to connect to a nationwide EHR registry.

In Germany most of healthcare providers have developed local EMR systems [15]. Currently, there is no single IT-system that connects all healthcare providers. The plan is to build eHealth infrastructure, which will enable nationwide communication between existing systems using standardized interfaces.

2.1.3. Turkey

Turkey EHR system has a centralized architecture. Turkey’s National Health Information System (NHIS) [16] provides a nationwide infrastructure for an EHR sharing. The aim of the system is to store all healthcare data from healthcare sites, scattered over the country, in repositories of Turkey Ministry of Health. It means that patient documents are stored mainly in local registries and their copy is send to a central registry. The NHIS built on the eHealth network, which connects basic components (National Health Data Dictionary (NHDD) and the Minimum Health Data Sets Server, Health Coding Reference Server, the digital security mechanisms). The HL7 v3 protocol is used for messaging purposes and web services for communication purposes. The NHDD is used to determine the format and definition of the data and thus enables semantic interoperability between different applications. The data flow is not only unidirectional, but also authorized persons have right to query and retrieve information from the central registry. In future, when necessary legislation will be passed, it will be possible to share clinical documents between healthcare providers.

2.2. IHE XDS

Almost all current EHR systems are built from many repositories and registries. IHE Cross-Enterprise Document Sharing (XDS) [17] profile provides specification based on established standards for managing the sharing of documents between any healthcare enterprises. The patient EHR is built from document repositories and from a document registry, where the document repository is responsible for storing documents and the document registry is responsible for storing metadata about those documents. Clinical documents are added to such system in a few steps. Firstly, the document is send to the repository (the repository can belong to document’ sender system or to the third party). Subsequently, the metadata is extracted from the document. Finally, the document identifier in the repository together with metadata is send to the registry. The healthcare professional can query the registry for patient’s clinical documents without the need of direct lookup to the clinical documents in one or more repositories.

2.3. Data storage location in national systems

International EHR system can span many national systems to provide better access to patient medical data. The main question in design of such system is where to store the EHR’s. There are three basic possibilities to store data: locally, centralized or hybrid. In local data storage all documents which belong to one patient are stored in many different local systems (hospital, laboratory, GP systems) and the documents are only registered in a central EHR systems registry, which stores only those documents metadata. In central data storage all medical documents are copied to a central EHR system repository. The hybrid data storage is a combination of both local and central data storage. From these systems, the most universal is a hybrid data storage system, because it provides more option to system developers. Security measures for such system, (presented further in this paper) can be also applied to a local or a central system.

EHR systems may have two types of registries: active and passive [19]. A passive registry acts like a telephone directory. A query to the registry returns the information about location of actual documents. An active registry acts like an information broker. The registry receives a query and propagates it to other registries or to other systems, which only registered the information in a central registry. The registry then collects the information and returns it to a query originator.

2.4. General model of an inter-jurisdiction EHR system

2.4.1. Documents’ sources

Clinical documents which are placed in an EHR comes from GP, laboratories, specialists, hospitals and any other healthcare sites and professionals participating in healthcare process. In an example scenario of allergy treatment, the patient visits his GP with allergy symptoms (the information about GP encounter is send to the EHR). Then patient is send to allergy specialist, before that patient visited laboratory for blood tests (laboratory specialist sends test results to the EHR). The specialist reads patient EHR, make some additional tests, diagnoses patient and give some prescription to the patient (test results, diagnoses and prescriptions are send to the EHR). Even a simple healthcare process involves many healthcare professionals, who place clinical documents in to the EHR. The professionals might work in different organizations and patients might go to them in different countries or regions, which might have different legal jurisdictions.

2.4.2. Model

A proposed general (hybrid) model of an inter-jurisdiction EHR system is presented in a figure 1. Healthcare professionals and subjects of care connect to the system by user access bus. The internal structure of the system is hidden from users. An Integrated Care EHR service stores information about all patients EHR’s. The service manages EHR’s in a long time period. It is able to provide to a query originator a view of an EHR in current or any previous points of time. It contains EHR index registry, which contains links to documents in repositories and to other registries and it contains location registry, which stores information about patients' records in other jurisdictions.

The clinical documents included in the EHR might be stored in:

- internal repositories and registries of the system – documents together with metadata are stored inside the EHR system;
- external repositories – the documents are stored in local HIS systems and are only registered in the EHR index registry; the external data bus with external information provider service mediate between the EHR system and a local HIS system;
- other EHR systems – documents with metadata are stored in other systems; the location registry stores only information if patients' records exists in that systems; the inter-jurisdiction bus mediate between EHR systems.

The Auxiliary systems bus mediate between the EHR system and systems indirectly involved in healthcare process e.g. visits registration system, epidemiological decision support systems or a PKI infrastructure for electronic signature support. Those systems are connected through specialized interfaces.

3. Security of proposed model

3.1. Security requirements

The general EHR system, which can be scalable up to any number of regions/countries have to deal with many security requirements. Implementation of those requirements for local systems, managed by a single organization, is usually trivial, but for an inter-organizational EHR system it becomes extremely complex. ISO TS 18308 [17] contains requirements for electronic health records architecture.

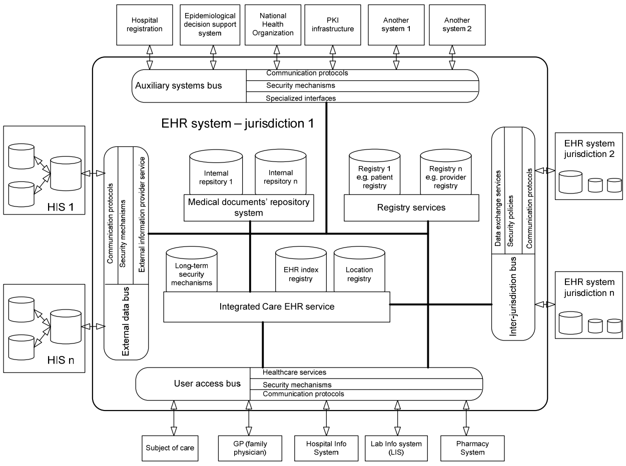

Fig. 1. A general EHR system
Rys. 1. Ogólny system EHR

According to ISO TS 18308 key issues related to the security of EHR architecture (EHR system) include authentication, data integrity, confidentiality, non-repudiation and auditablility. The requirements also include [17]:

- consent mechanism for access to parts or whole EHR;
- access control, which will support measures to define, attach, modify and remove access rights to the whole and/or sections of an EHR for classes of an EHR users;
- audit trail – access to and modifications of data within an EHR together with its nature should be recorded;
- version management – it should be possible to recreate an EHR representation in any previous point of time; documents should not be deleted;
- identification – the users who attest and commit information to an EHR should be uniquely identified, even if they change name, profession, address, etc.
- non-repudiation – every record entry should be dated and author should be identified.

A good review, based on a generic scenario questions, of the mentioned above EHR security issues were done by H. van der Linden et al. and is presented in [19].

3.2. Security measures

Security measures used in the EHR system can be divided into several separate mechanisms. A Figure 2 illustrates proposed security mechanisms. All communication with the system must go through appropriate buses, which have built-in security measures. All buses have auditing, secure transport and access control mechanisms. The user access buss has also consent mechanism. The inter-jurisdiction bus in addition has inter-jurisdiction security policy manager, which is responsible for security related problems connected to records exchange between different systems in different jurisdiction. Long-term security manager is inside the Integrated Care EHR service EHR and provides repository, registry security systems and also version manager.

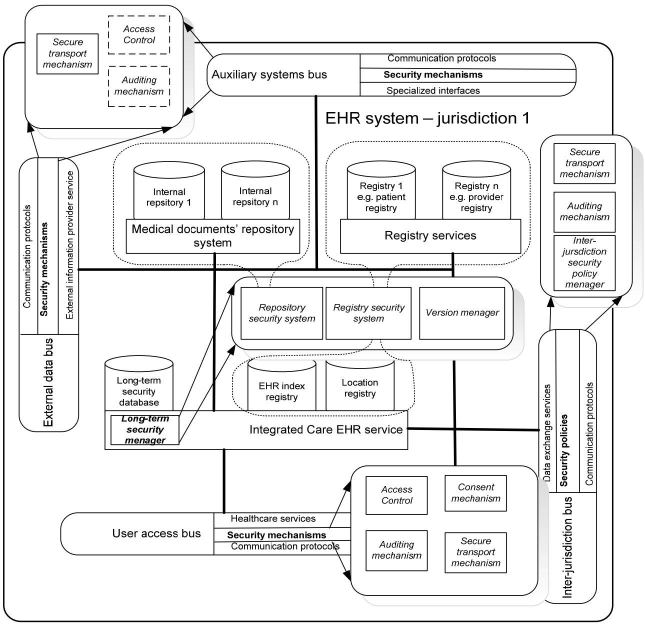

Fig. 2. Security measures for the EHR system
Rys. 2. Środki zabezpieczeń dla systemu EHR

The access control system is responsible for user authentication and authorization. The system is connected to consent mechanism, which manages patients consent to access to their EHR's. Also the system is responsible for emergency override option. The confidentiality is provided through that system. Auditing mechanism stores information about access to the EHR. Besides the need of checking who and when access some asset, it is sometimes necessary to check if someone did not look to the patient EHR during healthcare process. The secure network connections to external data sources and to other EHR systems are provided by secure transport mechanisms.

All clinical documents submitted to the patients EHR are digitally signed to ensure their integrity, authenticity and non-repudiation. A repository security system is responsible for maintaining digital signatures validity (the validity of digital signature is usually 2 years). The repository security system maintains documents without looking to their content. The function of maintaining the integrity of the EHR has a registry security system. The system allows checking if any document was added, changed or deleted from a patient EHR. A version manger collects information about version of documents and can restore the view of the EHR in any previous point of time, it is also responsible for notifying healthcare professionals if they seen incorrect version of clinical documents.

4. Summary and discussion

In this paper we have reviewed architectures of a few nationwide EHR systems. Based on that review, we have classified the systems by EHR documents' storage location: local, central or hybrid. The general model of the EHR system was created using this classification. The next step was to identify security requirements. EHR systems due to their complexity have many security requirements, which design and implementation is difficult in contrast to many modern information systems. We have presented security mechanisms for protection of the general EHR system, which will fulfil ISO/TS 18308:2004 requirements [18].

This paper does not describe details of security mechanism nor it show which solutions should be used to design them. We have proposed general building blocks of security mechanism and described their main purposes. The further work will be to design details of these security systems and test them against requirements.

5. References

[1] Bates D.W., Cohen M., Leape L.L., Overhage J.M., Shabot M.M., Sheridan T.: Reducing the frequency of errors in medicine using information technology. J Am Med Inform Assoc 2001; 8:299–308.

[2] Overhage J.M., Tierney W.M., Zhou X.A., McDonald C.J., A randomized trial of corollary orders to prevent errors of omission, J Am Med Inform Assoc 1997;4:364–75.

[3] Bates D.W., Evans R.S, Murff H., Stetson P.D., Pizziferri L., Hripcsak G.: Detecting adverse events using information technology, J Am Med Inform Assoc 2003;10:115–28.

[4] Bates D.W.: Using information technology to reduce rates of medication errors in hospitals, BMJ 2000;320:788–91.

[5] Jha A. K., Doolan D., Grandt D., Scott T., Bates D. W.: The use of health information technology in seven nations, Int. J. Med. Inform. 77 (2008) 848–854.

[6] Boulus N., Bjorn P., A cross-case analysis of technology-in-use practices: EPR-adaptation in Canada and Norway, Int. J. Med. Inform. (2008), doi:10.1016/j.ijmedinf.2008.06.008.

[7] Ludwick D.A., Doucette J., Adopting electronic medical records in primary care: Lessons learned from health information systems implementation experience in seven countries, Int. J. Med. Inform. (2008), doi:10.1016/j.ijmedinf.2008.06.005.

[8] Protti D., et al., Comparing the application of Health Information Technology in primary care in Denmark and Andalucía, Spain, Int. J. Med. Inform. (2008), doi:10.1016/j.ijmedinf.2008.08.002.

[9] Canada Health Infoway, http://www.infoway-inforoute.ca, last accessed: 22.04.2009.

[10] Canada Health Infoway, Corporate Business Plan 2008/09, online: http://www2.infoway-inforoute.ca/Documents/Infoway_Business_Plan_2008-2009_Eng.pdf, last accessed: 22.04.2009.

[11] Canada Health Infoway inc., A 'Conceptual' Privacy Impact Assessment (PIA) on Canada's Electronic Health Record Solution (EHRS) Blueprint Version 2, February 12 2008, online: http://www2.infoway-inforoute.ca/Documents/CHI_625_PIA_rj13.pdf, last accessed: 22.04.2009.

[12] House of Commons Health Committee ,The Electronic Patient Record Sixth Report of Session 2006–07, online: http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/422.pdf, last accessed: 22.04.2009.

[13] Rebane K.: eHealth in Estonia, online: http://www.epist.org/documents/balticIT&T/eHealth%20in%20Estonia.pdf, last accessed: 22.04.2009.

[14] Parre J.: Electronic Health Record Project of Estonia - Nation-wide Integrated eHealth Services, online: http://www.riigikantselei.ee/3qc/docs/ehealth/E_tervishoid_J_Parre_020904.ppt, last accessed: 22.04.2009.

[15] Gematik – Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, http://www.gematik.de, last accessed: 22.04.2009.

[16] Köse İ., Akpinar N., Gürel M., Arslan Y., Özer H., Yurt N., Kabak Y., Dogac A.: Turkey's National Health Information System (NHIS), online: http://www.srdc.metu.edu.tr/webpage/publications/2008/9.pdf, last accessed: 22.04.2009.

[17] ACC, HIMSS i RSNA, Integrating the Healthcare Enterprise (IHE), IT Infrastructure Technical Framework, Volume 1 (ITI TF-1) Integration Profiles, Revision 5.0 – Final Text, December 12, 2008.

[18] ISO/TS 18308:2004, Health informatics -- Requirements for an electronic health record architecture, TC 215, 2004.

[19] Linden H., Kalra D., Hasman A., Talomon J., Inter-organizational future proof EHR systems A review of the security and privacy related issues, Int. J. Med. Inform. 78 (2009) 141-160.

Artykuł recenzowany

INFORMACJE

Cennik publikacji artykułów technicznych

w miesięczniku naukowo-technicznym PAK

ARTYKUŁ TECHNICZNY	**w skali odcieni szarości** [ceny netto]	**kolor** [ceny netto]
Jedna strona	**500,00**	**700,00**
Dwie strony	**650,00**	**850,00**
Trzy strony	**800,00**	**1 000,00**
Cztery strony	**950,00**	**1 150,00**
pięć stron i więcej	**cena do indywidualnego uzgodnienia**	

Artykuł techniczny należy przygotować zgodnie z obowiązującymi wytycznymi znajdującymi się na stronie internetowej: www.pak.info.pl.