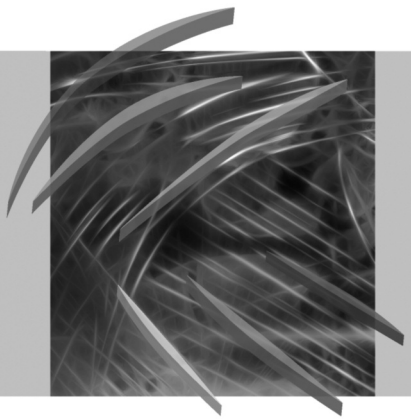
PRACE NAUKOWE
Uniwersytetu Ekonomicznego we Wrocławiu
RESEARCH PAPERS
of Wrocław University of Economics

205

Advanced Information Technologies for Management – AITM 2011

Information Systems in Business



edited by
Jerzy Korczak, Helena Dudycz, Mirosław Dyczkowski

Publishing House of Wrocław University of Economics
Wrocław 2011

Reviewers: Frederic Andres, Witold Chmielarz, Jacek Cypryjański, Beata Czarnacka-Chrobot, Bernard F. Kubiak, Wojciech Olejniczak, Celina M. Olszak, Marcin Sikorski, Ewa Ziemba

Copy-editing: Agnieszka Flasińska

Layout: Barbara Łopusiewicz

Proof-reading: Marcin Orszulak

Typesetting: Adam Dębski

Cover design: Beata Dębska

This publication is available at www.ibuk.pl

Abstracts of published papers are available in the international database The Central European Journal of Social Sciences and Humanities http://cejsh.icm.edu.pl
and in The Central and Eastern European Online Library www.ceeol.com

Information on submitting and reviewing papers is available on the Publishing House's website www.wydawnictwo.ue.wroc.pl

ISSN 1899-3192
ISBN 978-83-7695-178-2

The original version: printed

Printing: Printing House TOTEM

Contents

Streszczenia

PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU nr 205
RESEARCH PAPERS OF WROCŁAW UNIVERSITY OF ECONOMICS

Advanced Information Technologies for Management – AITM 2011 ISSN 1899-3192
Information Systems in Business

Daniel Wilusz, Jarogniew Rykowski
Poznań University of Economics, Poznań, Poland
e-mails: {wilusz; rykowski}@kti.ue.poznan.pl

THE ARCHITECTURE OF PRIVACY PRESERVING, DISTRIBUTED ELECTRONIC HEALTH RECORDS SYSTEM

Abstract: Electronic health records systems raised a great deal of controversy. On the one hand, immediate access to detailed patient's history improves medical procedures and may be even vital to patient's life. On the other hand, patient's health records usually contain very sensitive data which may be misused if not securely managed. The aim of this paper is to present architecture of an information system that preserves the privacy of patient's data by means of cryptographic techniques as well as proper cooperation among system participants. The main principle of the proposal is the assumption that entities know nothing more than is indispensible to them in order to fulfil their tasks.

Keywords: electronic health record, privacy protection, health information system.

1. Introduction

The electronic health records (EHR) systems seem to be a milestone in the development of medical information systems. The availability of complete and detailed patient history may be invaluable for the improvement of medical treatment. Moreover, the utilization of ICT and the development of telemedicine solutions is a milestone in the treatment of patients, as it allows remote diagnosis of a patient and a preparation of medical team in advance.

However, as pointed out in the literature, privacy issues of such systems and a need to protect sensitive patient data come to the attention [Choi et al. 2006; Kotz et al. 2009; Smith et al. 2010]. Moreover, some researchers claim that privacy issues are major inhibitor of the implementation of many EHR systems [Ray et al. 2006]. The survey conducted by Markle Foundation in U.S. indicated that over 80% of respondents believe that EHR systems would improve medical procedures and increase patient's consciousness about their health condition. On the other hand, about 60% of respondents expressed their concern about data privacy, and wished to have a possibility to manage the access to EHR on their own [Markle 2008]. Similar findings are shown by the survey conducted by A. Baird et al. [2011]. However, the

rate of concerns about privacy and security issues was higher in comparison with the Markle's survey and amounted to 91%.

The necessity to enhance patient privacy in EHR systems was expressed by I. Brown et al. [2011]. The authors listed the following problems of British national health system: not adequate information about secondary use of medical data, no request for patient consent, no option to opt-out, misleading about anonymous access to patient's data. What is more, Y.B. Choi et al. [2006] pointed out that benefits from using electronic health records "must not be accepted at the cost of individual privacy". Moreover, the importance of the respect for privacy is reflected in international law. For example, Article 12 of the Universal Declaration of Human Rights states that "No one shall be subjected to arbitrary interference with his privacy" [UN 1948]. Similar meaning has Article 7 of the Charter of Fundamental Rights of the European Union, which states that "Everyone has the right to respect for his or her private and family life" [European Parliament 2007].

There is a need for feasible information system, which would meet the needs of both patients and physicians. Such a system, on the one hand, should protect the privacy of patient, by allowing only him/her to decide about revealing his/her data. On the other hand, the physicians should be allowed to collect and analyze aggregated data about patients – so the information itself should not be encrypted. In addition, such a system should allow an emergency access to the patient's data. However, a decision about revealing medical data should be made by highly trusted person and each fact of data sharing should be recorded.

In this paper, a novel architecture of privacy preserving, distributed EHR system is presented. The cryptographic techniques, such as hash functions, symmetric and asymmetric cryptography are applied in order to assure patient privacy. The utilized techniques are carefully selected, so as to not affect the performance of patient's device which has limited computation capabilities (e.g., a smartcard).

To our best knowledge, not a single proposal has been published to allow access to medical data by means of the seeds and cryptography, with the grants related to patients' data rather than living persons (patients, physicians, administration personnel, etc.) and working at thin client approach. In the existing medical systems, usually a typical login/password-based approach is applied, aimed in the verification by means of user accounts, individual user grants, and access control lists to pieces of data. Moreover, in the existing systems a patient's card generates fixed identification number. No computation power of smartcard is utilized in order to identify health records instead of a patient.

The remaining of the paper is organized as follows. Section 2 describes system assumptions and participants. In Section 2.1, the process of physician enrolment is presented. Section 2.2 shows patient enrolment process. In Section 2.3, the EHR access protocol is carefully described, with particular emphasis put on security issues. Section 2.4 presents the process of a registration of a new electronic health record. Section 2.5 describes an access to the system in emergency situation. In Section 2.6

revocation of Anonymous Unique Identifiers is presented. Finally, Section 3 concludes the paper.

2. System architecture

In order to protect patient's privacy in the proposed system, the patient data are identified by Anonymous Unique Identifiers (AUIDs), which cannot be linked with particular patient. The AUIDs are generated by an application of a hash function to the seed and an encryption of the result with cryptographic function. Performing hash function recursively on the seed assures efficient generation of the unique (to some extent) AUIDs. However, as hash function is publicly known, the symmetric cryptography has to be applied, in order to assure unlinkability of AUIDs.

In order to assure the patient's privacy, the crucial roles such as data storage, certification, authorization and data access are divided among independent entities (Figure 1). Seven kinds of participants can be distinguished in the system: Patient, Physician, Central EHR access service, Hospital EHR Service, Certification Centre, Court, and City Hall. Each participant should be able to obtain only the information indispensable to fulfil their tasks.

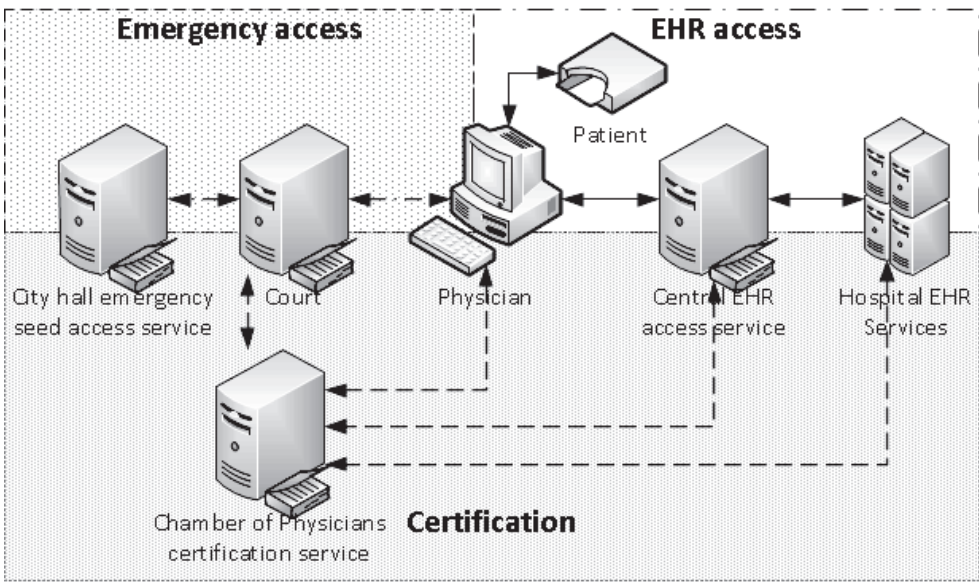


Figure 1. System participants

A *patient* is an actor who grants access to the electronic health records stored in the system by providing Anonymous Unique Identifiers to the physician. What is more, patient is the only subject (except emergency situation), who can identify

proper EHRs stored in the system. Additionally, the patient is the only actor generating AUIDs for newly created EHRs.

The *physician* should be able to access the patient data only if granted by a patient or by the court (in case of emergency) for limited time and within the scope of his/her specialty. The AUIDs are not revealed to the physician, but provided in an encrypted form, as this information is not indispensible to this actor. A physician is a semi-trusted party – it is assumed that any physician will not misuse the content of EHRs.

Central EHR access service allows the localization of EHRs stored in distributed databases of particular hospitals. In order to enable efficient localization of AUIDs related with the medical data, this entity stores the relations among AUIDs and hospital EHR services where health records are stored. However, this entity does not know the patient's identity and the content of patient related EHRs.

Hospital EHR service provides EHRs to the certified physicians who have been granted by the patients to access their medical records. This actor assures that only certified physicians may obtain patient data and only within the scope of their access rights stated in the access certificates. As the system assumes a dispersion of Hospital EHR service providers, the linkage of patient with EHRs is unlikely.

Chamber of Physicians acts as the certification centre, which certifies public keys for physicians, Central EHR access service, Hospital EHR Services and Court (judges). In order to avoid adversary attack, the Chamber allows checking credibility and data access scope of entities accessing the system.

City Hall is the actor responsible for preparing patient access device (i.e., smart card) and generating the seed – the base for generation of AUIDs, however, the seed alone is not sufficient to generate AUIDs. In the case of emergency situation, this entity is obliged to provide particular seed to the Court, if requested.

Court plays significant role in emergency access to EHRs. This actor is entitled to generate patients AUIDs and grant access to medical data in case of emergency.

2.1. Physician enrolment

The enrolment of a physician to the proposed EHR system is carried out by Chamber of Physicians. In order to access EHR system, physician requests the Chamber for the certificates enabling the identification and authorization in the system. After a verification of physician personal details and medical specialties, Chamber of Physicians decides if to grant an access to the system and which authorization level should be granted.

After positive verification, the Chamber certifies physician public key (*phyKp*) and issues authorization certificates specifying types of medical data which can be accessed by a particular physician. For security reasons authorization certificates are valid by limited time and should be temporarily renewed.

2.2. Patient enrolment

In the proposed EHR system, the cooperation with public administration is needed in order to enrol a patient. By default, each patient is enrolled to the system during the process of issuing his/her ID card. The patient enrolment process is presented in Figure 2.

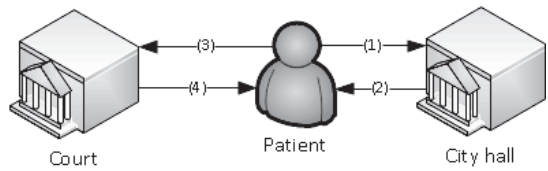


Figure 2. Patient enrolment

In the first step, a patient fills application for ID card at City hall (1). Next, the City hall prepares ID card enabling the use of EHR system. The main role of the software operating in ID smart-card is to generate Anonymous Unique Identifiers (AUIDs). City hall generates seed – the bit string which is indispensable to generate AUIDs. In order to avoid collisions and adversary attack, every patient should obtain a seed of different value. The seed should be also difficult to guess by any adversary. To assure the above mentioned requirements, the seed consists of the concatenation of the server ID, a timestamp and randomly generated bit string (*seed* = *serverID*||*timestamp*||*rand*). The seed is stored in City Hall database for the purpose of emergency access. Additionally, City Hall stores in ID card the public key of Central EHR Access service (*ceasKp*). Next, the City Hall provides EHR enabled ID card to the user (2).

After receiving his/her ID card, a patient generates symmetric cryptographic key (*patCK*), which is used during generation of AUIDs. Next, patient sends *patCK* to the court in order to enable emergency data access and to have a possibility to restore the AUIDs in the case when accessing device is lost (3). Finally, the court stores the key in the database and confirms successful operation (4).

2.3. Access to electronic health records

In order to preserve patient privacy and assure access control, five entities are engaged in EHR access protocol (Figure 3). The process of access to the EHRs consists of eight phases and is described below.

In the first step, physician asks a patient to insert his/her ID card in the physician's card reader and to provide PIN code (1). Next, the software installed in ID card performs following operations:

- establishes communication with physician's terminal,
- requests for physician public key (*phyKp*),
- generates random cryptographic key of particular length (*patRK*),

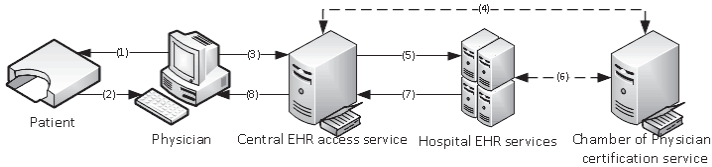


Figure 3. Access to electronic health records

- encrypts concatenation of *patRK*, timestamp (*TSP*) and *phyKp* with public key of Central EHR access service in order to generate a grant of access $GRANT = ceasKp(patRK||TSP||phyKp)$),
- sends *GRANT* to the physician,
- gets from memory the number of already generated AUIDs (n) and *seed*,
- begins the loop calculating and encrypting the AUIDs:
  - $AUID_i = patCK(H^i(seed))$ where *patCK*() is cryptographic function with symmetric key *patCK*, and i is the number of loop iterations such that $1 \leq i \leq n$. $H^i(seed)$ means performing hash function on seed i times (e.g. $H^3(seed) = H(H(H(seed)))$);
  - $EAUIDi = patRK(AUIDi)$ where *EAUIDi* is *AUIDi* encrypted with symmetric key (*patRK*). This encryption prevents from revealing the AUIDs to the physician as well as from eavesdropping by adversary;
  - Sends *EAUIDi* to the terminal,
- ends data exchange with the terminal (2).

In the next phase, physician's EHR access software prepares package in the form of $PACK = \{GRANT, EAUID_1, EAUID_2, \ldots, EAUID_n\}$. This package, together with physician's certificates, is sent to the Central EHR access service (3).

After receiving request to provide access to the patient's data, Central EHR access service performs following security checking steps:

- decrypts *GRANT* in order to check validity of request,
- verifies the physician's public key certificate at Chamber of Physicians certification service (4)

If security checking process is passed, Central EHR access service proceeds to further steps:

- decrypts EAUIDs with *patRK* and finds Hospital EHR services storing patient related data;
- prepares for every Hospital EHR service storing patient data, the EHR request package in form of $ERPACK_a = \{phyKp, AUID_{a1}, AUID_{a2}, \ldots, AUID_{ak}\}$ where a is a number of Hospital EHR service storing patient related data, k is the number of patient related records in particular Hospital EHR service, $a1, a2, \ldots, ak \in \langle 1;n \rangle$ and $k \leq n$;

- sends ERPACKs and physician's certificates to the particular Hospital EHR services (5).

Hospital EHR service, when obtaining package from Central EHR access service, performs the following steps:

- verifies physician authorization certificates at Chamber of Physician certification centre in order to determine data access scope. Especially, certificates are compared with revocation list (6),
- searches database for electronic health records identified by AUIDs,
- picks EHRs matching physician's access scope,
- generates random cryptographic key for symmetric encryption (*hesRK*),
- encrypts *hesRK* with physician's public key – *phyKp*(*RK*),
- encrypts EHRs with random key – *RK*(*EHR*),
- prepares EHR package in form of $EHRPACK = \{phyKp(RK), RK(EHR_1), RK(EHR_2), \ldots, RK(EHR_m)\}$ where $m \leq n$,
- stores the fact of physician access to health records in database,
- sends *EHRPACK* to Central EHR Access Service (7).

In the next phase, the Central EHR access service collects the EHRPACKs from Hospital EHR services and forwards them to the physician (acting as a multiplexer and transparent proxy) (8).

After receiving EHRPACKs, the physician decrypts *hesRK* by using his/her private key and then decrypts electronic health record. Next, EHRs are grouped in order to present patient's medical history.

2.4. Registration of new electronic health record

The proposed system allows a physician to register a new EHR. In order to store diagnosis in the system, the physician cooperates with the patient and Hospital EHR service. The process of EHR registration is presented in Figure 4.

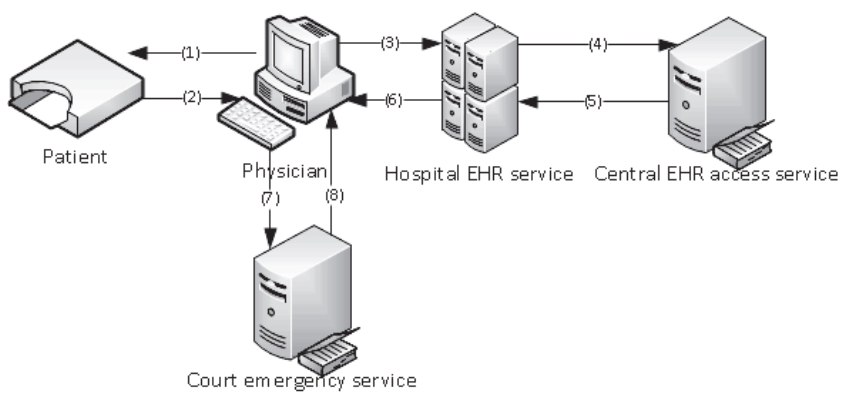


Figure 4. Registration of a new electronic health record

After writing the diagnosis, the physician's software creates the digest of this diagnosis, by performing hash function on new *EHR* (*DIGEHR* = *H*(*EHR*)). The digest of diagnosis aims in assuring data integrity. Next, the physician sends to the patient's ID card the certified public key of Hospital EHR service (*hesKp*) with *DIGEHR* and requests generation of new AUID (1).

In turn, the software stored on patient's card performs following operations:

- verifies certificate of Hospital EHR service public key,
- gets from memory the number of already generated AUIDs (*n*) and *seed*,
- performs hash function on *seed* $n + 1$ times and encrypts result with *patCK* in order to generate new AUID ($AUID_{n+1} = patCK(H^{n+1}(seed))$),
- signs value of $n + 1$ to *n* and stores it in memory,
- encrypts $AUID_{n+1}$ concatenated with *DIGEHR* using *hesKp* (*hesKp*($AUID_{n+1}$||*DIGEHR*)) and sends the result with *n* to the physician (2).

Next, the physician's software executes following operations:

- generates random cryptographic key (*phyRK*),
- encrypts *phyRK* with *hesKp*,
- encrypts *EHR* with *phyRK*,
- prepares package in form of *NAPACK* = {*hesKp*($AUID_{n+1}$||*DIGEHR*), *hesKp*(*phyRK*), *phyRk*(*EHR*)} and sends it to Hospital EHR service (3).

After receiving NAPAC, Hospital EHR service performs following steps:

- decrypts *hesKp*($AUID_{n+1}$||*DIGEHR*), *hesKp*(*phyRK*) and *phyRk*(*EHR*),
- performs hash function on EHR and compares with DIGEHR (*H*(*EHR*) = *DIGEHR*)),
- dtores *EHR* identified by $AUID_{n+1}$ key in database,
- generates localization package (*LOCPACK*) by encrypting concatenation of $AUID_{n+1}$ with own ID (*hesID*) using *ceasKp* (*LOCPACK*=*ceasKp*($AUID_{n+1}$||*hesID*)),
- sends *LOCPACK* to the Central EHR access service (4).

In the next step, the Central EHR access service decrypts *LOCPACK*, stores the relation $AUID_{n+1} \rightarrow hesID$, and confirms this operation (5). After receiving a confirmation from Central EHR access service, the Hospital EHR service sends to the physician a confirmation of successful operation (6). Then the physician sends *n* (the current number of generated AUIDs) to the Court emergency service for emergency access purposes (7). After the Court confirms the update of *n*, the registration of a new EHR record ends (8).

2.5. EHR emergency access

The proposed system assumes that a situation may happen when a patient is unable to provide AUIDs or the patient's device is lost. To solve this problem, an emergency access is proposed. The phases of EHR emergency access are presented in Figure 5.

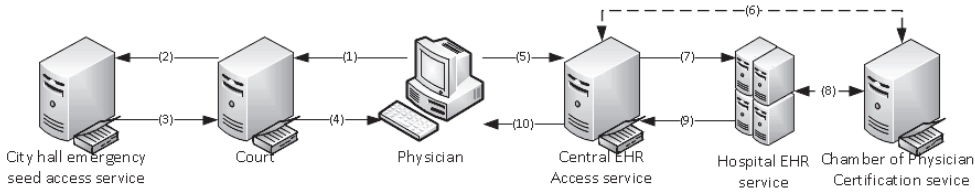


Figure 5. EHR emergency access

In the case of emergency situation, when patient's health status does not allow performing necessary steps to use the system, the physician may contact the court to begin EHR emergency access procedure. The physician requests an access to the patient's EHRs by sending to the court a description of the patient's health status, own public key and authorization certificates (1). A judge considers physician's request, and if conditions to provide patient's data are met, grants the access to EHRs. In order to allow the physician to access patient data, the court has to generate patient's AUIDs. The court requests the seed from City hall emergency seed access service (2). Then City hall stores the fact of court's request in the database and provides the seed (3). Next, the court generates the package of AUIDs in following steps:

- generates random cryptographic key of particular length (*courtRK*),
- encrypts concatenation of *courtRK*, timestamp (*TSP*) and *phyKp* with public key of Central EHR access service in order to generate grant of access $GRANT = ceasKp(courtRK||TSP||phyKp)$),
- gets patient's symmetric cryptographic key (*patCK*) and number of already generated AUIDs (*n*) from database,
- begins the loop calculating and encrypting the AUIDs
  - $AUID_i = patCK(H^i(seed))$;
  - $EAUIDi = courtRK(AUIDi)$,
- prepares package in form of $PACK = \{GRANT, EAUID_1, EAUID_2, \ldots, EAUID_n\}$ and sends it to the physician (4).

The physician after receiving PACK is able to access the patient's EHRs in the system. The phases 5 to 10 are the same as phases 3 to 8 of the access to electronic health records described in Section 2.3.

2.6. Revocation of AUIDs

After emergency access, patient is able to revoke AUIDs revealed by the court. The patient contacts the City Hall in order to obtain *newSeed*, then generates new cryptographic key (*newPatCK*), and sends it to the court. Next, he/she contacts the hospital and generates *REVPACK* in form of $REVPACK = \{ceasKp(patRK), EAUID_1, EAUID_2, \ldots, EAUID_n\}$ and *NEWPACK* in form of $NEWPACK = \{H(REVPACK), patRK(newPatCK(H(newSeed))), patRK(newPatCK(H^2(newSeed))), \ldots, patRK(newPatCK(H^n(newSeed)))\}$. The hospital, after receiving *REVPACK* and *NEWPACK* requests, asks Central EHR access service to replace old AUID with new

ones. The Central EHR access service decrypts REVPACK and NEWPACK, localizes particular Hospital EHR services and requests them to replace old AUIDs with the new ones. After the replacement, Hospital EHR service confirms the successful operation to the Central HER access service and this confirmation is forwarded to the hospital. An execution of these steps re-assures complete patient's privacy.

3. Conclusions and future work

In this paper a novel architecture of the electronic health records distributed system was presented. The architecture aims at preserving patient's privacy, assuming that a functionality of nowadays medical systems is preserved. The main achievement of this paper is the presentation of genuine protocol for the generation of anonymous unique identifiers. Moreover, the choice of system actors, links among them and cryptographic techniques applied in communication protocols minimizes the risk of patient's data leakage. Especially distribution of hospital EHR services causes that patient's data are not stored in one database but are dispersed among particular hospitals' information systems. This approach minimizes the risk of compromising patient's anonymity by utilization of data mining techniques.

The authors are conscious about possible privacy threats, which may be caused by the misuse of court power – a judge is able to take a decision to somehow "bypass" the system restrictions to access any patient's data. However, the judges are the citizens of the highest trust. An implementation of a prototype of the proposed approach is ongoing by means of smart cards, smartphones, and short-range wireless communication (particularly NFC). As the future work, we plan to achieve anonymous access to medical data (anonymous medical treatment) with full respect to the patient's privacy, and (at least) nowadays level of overall system functionality (i.e., no data restrictions caused by the fact of anonymity).

The proposal is not restricted to medical systems. However, we found that these systems strongly need improved authorization methods, capable of the support for incidental contacts between a patient and a physician, and respecting data privacy. Thus, we applied our proposal to the medical systems at first. However, we see some other possible application areas of our authorization scheme, such as anonymous payments (a client provides AUID instead of bank account number in order to prevent tracking by a merchant) or electronic administration (to prevent clerks from accessing information, which is not indispensable to fulfil their tasks).

References

Baird A. North F., Raghu T.S. (2011), Personal Health Records (PHR) and the future of the physician-patient relationship, [in:] *iConference '11 Proceedings of the 2011 iConference*, ACM, New York, pp. 281–288.

Brown I., Brown L., Korff D. (2011), Limits of anonymisation in NHS data systems, *British Medical Journal*, 2011 Feb 22; 342:d973.

Choi Y.B., Capitan K.E., Krause J.S., Streeper M.M. (2006), Challenges associated with privacy in health care industry: Implementation of HIPAA and the security rules implementation of HIPAA and the security rules, *Journal of Medical Systems*, Vol. 30, No. 1, Springer Science+Business Media, pp. 57–64.

European Parliament (2007), Charter of Fundamental Rights of the European Union, *Official Journal of the European Union*, C303 Vol. 50, 14 December 2007.

Kotz D., Avancha S., Baxi A. (2009), A privacy framework for mobile health and home-care systems, [in:] *SPIMACS '09 Proceedings of the First ACM Workshop on Security and Privacy in Medical and Home-care Systems*, ACM, New York, pp. 1–12.

Markle (2008), *Technology Companies, Providers, Health Insurers and Consumer Groups Agree on Framework for Increasing Privacy and Consumer Control over Personal Health Records*, http://www.markle.org/news-events/media-releases/technology-companies-providers-health-insurers-and-consumer-groups-agree (accessed 13.06.2011).

Ray P., Wimalasiri J. (2006), The need for technical solutions for maintaining the privacy of EHR, [in:] *Engineering in Medicine and Biology Society, 2006. EMBS '06. 28th Annual International Conference of the IEEE*, IEEE, pp. 4686–4689.

Smith B., Austin A., Brown M., King J.T., Lankford J., Meneely A., Williams L. (2010), Challenges for protecting the privacy of health information: required certification can leave common vulnerabilities undetected, [in:] *SPIMACS '10 Proceedings of the Second Annual Workshop on Security and Privacy in Medical and Home-care Systems*, ACM, New York, pp. 1–12.

UN (1948) *Universal Declaration of Human Rights*, http://www.un.org/en/documents/udhr/ (accessed: 30.11.2011).

ARCHITEKTURA CHRONIĄCEGO PRYWATNOŚĆ, ROZPROSZONEGO SYSTEMU INFORMACJI O PACJENCIE

Streszczenie: Elektroniczne systemy informacji medycznej wzbudzają wiele kontrowersji. Z jednej strony dostęp do szczegółowej historii choroby pacjenta z pewnością poprawia sposób leczenia, a w niektórych przypadkach może uratować życie. Jednak z drugiej strony informacje medyczne o pacjencie należą do danych wrażliwych i mogą zostać nadużyte, jeśli system informacji medycznej nie jest odpowiednio zaprojektowany. Celem niniejszego artykułu jest zaprezentowanie architektury systemu informatycznego, który pozwala na zapewnienie prywatności danych pacjenta przez zastosowanie technik kryptograficznych oraz odpowiedni dobór podmiotów i powiązań między nimi. System został zaprojektowany według zasady, że podmioty uczestniczące w wymianie informacji nie wiedzą więcej, niż jest im niezbędne do poprawnego wykonania ich zadań.