Privacy-aware Access to Patient-controlled Personal Health Records in Emergency Situations

Md. Nurul Huda, Shigeki Yamada, and Noboru Sonehara
National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo, Japan
{huda, shigeki, sonehara}@nii.ac.jp

***Abstract*— Patient-controlled Personal Health Record (PHR) systems may facilitate a patient not only to share her health records with healthcare professionals but also to control her health privacy, in a convenient and easy way. Governed by privacy protection laws, explicit consent/permission of the respective patient is a prerequisite for sharing personal health records. However, in emergency situations, when the patient becomes unable to give consent on her PHRs, healthcare professionals of emergency care units may need to access her health history for better and safer care. In this paper, we have introduced a novel privacy-aware protocol for handling access to patient-controlled PHR by healthcare professionals in emergency situations. The protocol is for the Privacy-aware Patient-controlled Personal Health Record (P^{3}HR) system . It uses strong authentication using health IC cards, authorizes healthcare professionals and embeds emergency access report into the patient's health IC card by which we achieve non-repudiation. Use of a dynamic access token in the authorization process protects replay attack. Intuitive privacy analysis shows that the proposed solution can preserve patient's privacy from unauthorized parties while granting traceable access to personal health records by authorized healthcare professionals in emergency situations.**

Keywords-Personal health record, privacy, emergency access, healthcare service.

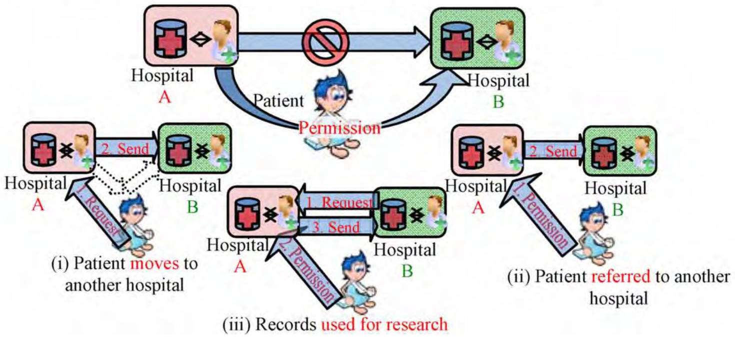
I. Introduction

Patients sometimes may need to get healthcare services from different healthcare centers, other than their regular care centers, for various reasons such as unavailability of service on holidays, need for specialized care at specialized centers, travelling away from residence area, and changing residency [1]. However, in traditional healthcare systems, the stored health information in a healthcare center is usually accessible only to authorized healthcare personnel of that center [2]. For every healthcare center, there are separate systems to record patients' health information, and information flow between systems is very limited.

Privacy protection laws restrict open access to personal health records from one healthcare center to another. As illustrated in Fig. 1, the healthcare center, which is storing certain health records of a particular patient, must acquire written permission (as a proof of consent) of the respective patient before dispatching personal health records of that patient to a different healthcare center. Thus, in these systems, it might be inconvenient (and sometimes impossible) to get necessary health history of a patient that could be very important for her safer treatment.

Each time a patient visits a new healthcare center, she may need to request for her old health records from several previously visited healthcare centers, which is a time consuming and tedious job. Health smart cards [3] can help make health care safer, cheaper, and more convenient allowing healthcare professionals to have immediate access to PHRs anytime anywhere[4][5]. However, for the sake of privacy protection, patients should have the control over their personal health records. Thus, the necessity of a patient-controlled personal health record system has been felt by many researchers [1][6-9][10]. In such a system, the patient can fully control her privacy and share the desired part of her health information with specific healthcare professional when desired.

Patient-controlled PHR should have emergency situation handling capabilities. Let us consider the scenario where Alice has been seriously injured in an accident and became unconscious. She has been taken to the emergency care unit of a nearby hospital where there is no health information about her. Before applying a particular drug into Alice's body, the doctor needs to know if she has diabetes. Getting health history from other hospitals might be impractical (because of privacy protection laws) or even be impossible (because it is not known



(i) Patient moves to another hospital

(iii) Records used for research

(ii) Patient referred to another hospital

This project was financially supported by the Japan Society for the Promotion of Science (JSPS).

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.6008
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.6008

which other hospitals possibly storing her health information). Had Alice been not unconscious, the doctor could get the required information from her personal health record system, which is controlled by Alice herself. Thus, we need the technology that not only supports general privacy protection but also provides mechanism to make the desired PHR available to the appropriate healthcare professionals in emergency situations.

Privacy awareness in patient-controlled PHR is an important issue and we have thoroughly discussed it in paper [10]. In this paper, we focus on privacy issues in emergency situations where the patient is unable to give consent interactively but healthcare professionals need to access PHRs for life saving. A privacy-aware solution should not only make the necessary health information available to the healthcare professional in emergency situations but also report non-reputable access trace to the patient.

The rest of the paper is organized as follows; in section II we briefly present related works with a special focus on P^{3}HR system, which is the basis of the devised protocol presented in the paper. Section III describes the protocol in details. Section IV analyzes the security and privacy issue to show its characteristics. Finally, section V concludes the paper with discussion.

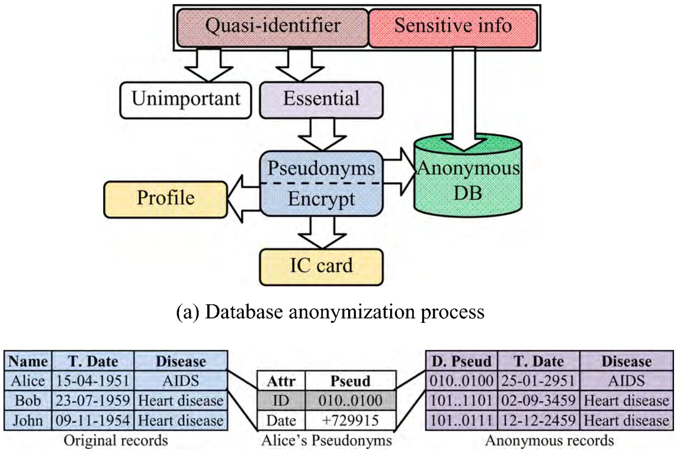
II. Related Work

Much of the background for the discussion in this paper comes from the P^{3}HR system [10]. In this section, we briefly describe the P^{3}HR system with a focus on the privacy control model. The information presented in this section serves as a basis for further discussion in the remainder of this paper.

A. *P^{3}HR*

In our P^{3}HR system the patients control who would be allowed to access which part of their health records and for what duration. It has an online database of personal health records where no quasi-identifier values [12][13] are stored. Essential quasi-identifiers values that are important for health history (e.g., prescription date) are replaced with patient created pseudonyms. Fig. 2(a) depicts database anonymization process in P^{3}HR system with a brief example. A patient creates her unique digital pseudonym [13][14] and pseudonyms for the quasi-identifiers that must be kept in the database for accurate health history. The pseudonyms are encrypted into her health IC card and her profile. Instead of storing the quasi-identifier values, their pseudonyms are stored into the database making the database anonymous.

Patient created unique digital pseudonyms are appended with each record when a patient accepts new records into her personal health records. This pseudonym is used to link a record with its associated patient when the record is read. The resulting database becomes most likely completely anonymous. Unlike *k*-anonymity [15] or *l*-diversity [16] method, attribute values of a record are not generalized or modified and hence the accuracy of the stored data is preserved. Fig. 2(b) shows a sample original and anonymous health records. Alice created her digital pseudonym (ID) and a date pseudonym. Her digital pseudonym was added with her records and date values of her records were replaced according to her date pseudonym resulting in anonymous record.



(a) Database anonymization process

Name	T. Date	Disease
Alice	15-04-1951	AIDS
Bob	23-07-1959	Heart disease
John	09-11-1954	Heart disease

Original records

Attr	Pseud
ID	010..0100
Date	+729915

Alice’s Pseudonyms

D. Pseud	T. Date	Disease
010..0100	25-01-2951	AIDS
101..1101	02-09-3459	Heart disease
101..0111	12-12-2459	Heart disease

Anonymous records

(b) Example of anonymizing records

Figure 2. Database anonymization in P^{3}HR system.

The pseudonym of a patient is kept encrypted into her profile and is used to calculate back the original information when the patient views her own health records online from home. The same pseudonyms are also stored encrypted into her health IC card that is needed when a healthcare professional wants to view a patient’s health information from a hospital. Fig. 3 illustrates the process of reading PHRs of a particular patient from her home and a visited hospital.

The patient’s pseudonym is known to the respective patient only and does not need to reveal even to the healthcare professionals who access her anonymous health records with the help of the patients’ health IC card. Even if the records are exposed to unauthorized parties, it is very unlikely that they would identify the respective patients from their anonymous health records because no quasi-identifiers are stored into the database and the pseudonyms are secret. Thus, in P^{3}HR the patients’ privacy is preserved from unauthorized parties.

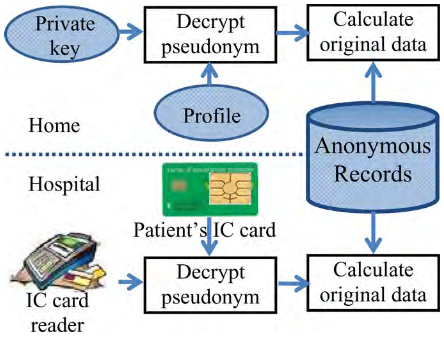


Figure 3. PHR reading method in P^{3}HR.

B. *Other Related Works*

The Indivo [7] is the world's first patient-controlled web-based record system, enabling a patient to own a complete,

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.6008
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.6008

secure copy of her medical record, integrating health information across multiple care centers. Google and Microsoft launched Google Health [8] and HealthVault [9] respectively. They allow individual to store and manage all of his/her health information in one central place. One can import his health records from his doctors, hospitals, labs, prescription drug plans, and other healthcare providers. There are several other implementations of patient-controlled health record systems that facilitate patients to share their health records with healthcare professionals. National Health Service (NHS) of UK [17] is evolving toward a comprehensive electronic record that provides secure and accessible health information to professionals and patients across the nation. iHealthRecord [18], was designed to facilitate online access to information and care. Patients retain control and responsibility to initiate their own iHealthRecord. It improved access to records and share them with others in a more convenient way.

Above health record management services vary in the type of utilities/services that they offer and the extent the patients get control over their health records. The main limitation of all of the existing works is that they are not strongly privacy-aware. An intruder, who gets access to the health database, can easily de-identify a patient from the attribute that links the records with specific individuals. So, they do not support strong privacy control. Also, they do not provide a mechanism of managing access to PHRs in emergency situations.

The Break-Glass [19] approach is based upon pre-staged "emergency" user accounts, managed in a way that can make them available with reasonable administrative overhead. It grants emergency access to Healthcare systems and is appropriate for the systems where the operator can get access by supplying only username and password. It is merely an access control issue and is suitable for hospitals' local healthcare systems in which a patient can be identified from the records.

Although the health smart cards implemented in many Western European countries and some Asian countries allow emergency access to the PHRs that are stored in the card themselves, those card systems do not support strong and flexible privacy control. Any doctor, having a medical professional smart card, can read most of the data from a patient's health smart without the patients' consent.

III. Emergency Accesst

Emergency access to PHRs in our proposed method involves several phases such as authentication/identity verification, authorization, access, report and cleanup. Following, we describe each of the phases. It is assumed that the patient's health IC card, doctor's IC and card reader are available at the hospital. Also, the card reader software can connect to the internet

A. Authentication/identity varification

Data stored on the IC cards cannot be read without going through a strict authorization and mutual authentication process. The security access module of the card reader verifies the identity of healthcare professional cards and patient cards. The card reader and the card authenticate each other through mutual dynamic symmetric authentication using a challenge response method. Only after doctor presents his own medical professional IC card, his card and patient's card verify each other. After cross-verification the card reader can read the content of patient's IC card. The authentication of the healthcare professional is verified through passwords system.

B. Authorization

In P^3HR system, patient cards keep digital pseudonym of the patient that associate her health records in the database. In normal operation, the patient herself authorize the doctor to access her health records by PIN number, which can decrypt her digital pseudonym form her card and the application sends the access request for the records with the decrypted digital pseudonym. But in emergency situations, it is assumed that the authorization cannot be given interactively by the patient. The patient IC card has an emergency access module that handles emergency access. The emergency access module has a dedicated rewritable memory portion for storing emergency access digital pseudonyms and emergency access token (EAT) which is generated as a function of a random number and unique user identification. The dedicated memory space is used for writing emergency accessing doctor's identification information. A token can be used by only one doctor and a new token is set when emergency access report is cleaned up. The EAT is also stored with the profile of the patient at the P^3HR server. Following steps take place for authorizing emergency access in P^3HR. Fig. 4 illustrates the authorization sequence diagram.

1. The doctor's card sends emergency access request along with the doctor's identification information to the patient card through the emergency access unit.
2. The patient's card and the doctor's card mutually authenticate each other.
3. The patient card reads EAT and emergency access pseudonyms into its RAM.
4. The patient's card checks if current requesting doctor's information exists into its dedicated memory.
5. If the doctor's info is present into the dedicated memory, the EAT and the emergency access pseudonyms are flashed out and the requesting doctor's info is written into the dedicated memory. However, if the doctor's info exists into that memory, the access is denied. A corresponding reply is sent to the emergency access module.
6. Again the emergency access module checks whether the current requesting doctor's information exists into the patient card's dedicated memory.
7. If the information is found there, the patient's card sends the pseudonyms and the emergency access token to the emergency access unit which then uses them to send access request to the P^3HR server.
8. The authorization is checked at the server through the emergency access token and the pseudonyms are used to

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.6008
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.6008

retrieve only the records related to the patient of the card holder.

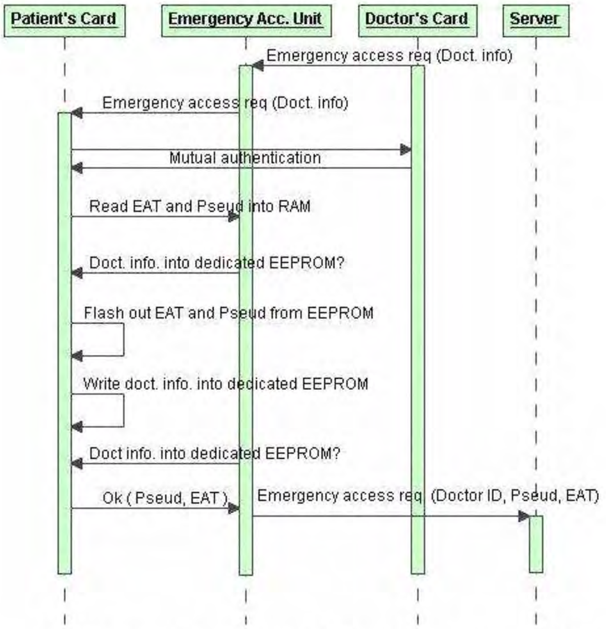

Patient's Card
Emergency Acc. Unit
Doctor's Card
Server
Emergency access req (Doct. info)
Emergency access req (Doct. info)
Mutual authentication
Read EAT and Pseud into RAM
Doct. info. into dedicated EEPROM?
Flash out EAT and Pseud from EEPROM
Write doct. info. into dedicated EEPROM
Doct info. into dedicated EEPROM?
Ok (Pseud, EAT)
Emergency access req (Doctor ID, Pseud, EAT)

Figure 4. Authorization protocol for emergency access in P^{3}HR.

It is assumed that the emergency access is necessary for short duration (i.e. one session). Once emergency access is carried out by a doctor, the dedicated memory is occupied with the doctor's identification information and the emergency access token and the pseudonyms that were previously stored there are lost. A card can be set to few numbers of emergency accesses with separate emergency access tokens for each of them. If an emergency patient is transferred from one hospital to another, the card still can be used by several doctors, determined by the number of EAT. When all of the EATs are used by different doctors, the card cannot be used further for emergency access until the patient resets the card's dedicated memory with new access tokens through her password.

C. Access

Authorized doctor's requests allow the emergency access unit to retrieve the pseudonym and emergency access token from the patient's IC card. However, the retrieved pseudonym and the token are not visible to the doctors. They are used internally by the emergency access unit to send access request to the server.

All access requests go through the privacy control module of the P^{3}HR system. The personalized privacy control module stores a copy of the emergency access token (EAT). It checks whether the value of the EAT, which comes with the emergency access request, is the same as that of the locally stored EAT. If they match with each other, the privacy control module allows access to the PHRs that are related to the digital pseudonym that came with the emergency access request. The privacy control module logs the emergency access information and creates a special report for the patient. Fig. 5 depicts the emergency data access protocol in P^{3}HR.

A healthcare professional can use a patient's card for emergency access only once because the EAT value that is checked by the privacy control module get lost as soon as the patient's card is taken out of the card reader. Also, a patient's digital pseudonym cannot be retrieved from her profile at the server. Any intruder without the patient's health IC card cannot determine her digital pseudonym and thus cannot associate anonymous health records with the patient.

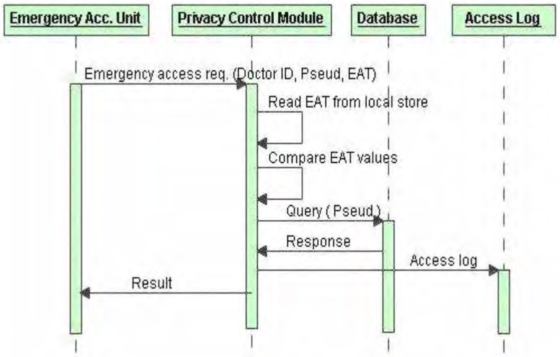


Figure 5. Emergency data access protocol.

D. Report

Since, there is no scope of getting direct consent of the patient during emergency access and getting indirect consent through the patient pre-assigned proxy may cause unexpected delay, the privacy awareness strictly demands report of the emergency access to the patient as soon as possible. To confirm the reporting, the authorization protocol stores the accessing doctor's identification information into the patient's card which cannot be reset by anyone except the patient himself (with his password). The access information is also stored into the P^{3}HR server's access log in the emergency data access protocol. The use of the doctor's IC card and inclusion of the doctor's information with the emergency access request by the emergency access unit ensures that the actual doctor's information is stored into the patient's access log at the P^{3}HR server. The accessing doctor may report the emergency access explicitly. Even if not, the patient gets notified as soon as she checks her card or checks her online profile.

E. Cleanup

Cleaning up involves acknowledging the recorded emergency accesses and resetting the required parameters for the next emergency access. It requires card owner's authentication. Following steps take place in the reset procedure:

1. The patient makes a reset request to the emergency access module.
2. It asks the password for authentication. When supplied, it shows the last emergency accessed doctor's identification information.
3. It creates new emergency access token (EAT) and decrypts the patient's digital pseudonyms.

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.6008
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.6008

4. It flashes out recorded accessing doctors identification information and overwrites the dedicated memory space with the patient's digital pseudonyms and the new emergency access tokens (EAT).
5. The patient's card also sends the new emergency access tokens (EAT) to the patient's profile at the P^3HR server which updates the emergency access token with the new value.

Fig 6 shows the protocol for resetting emergency access data.

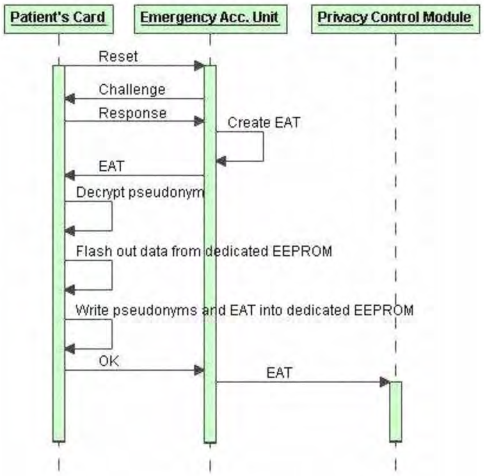


Figure 6. Resetting emergency access data

IV. Privacy Characteristics

We assume that the described policies are enforced by the trusted service provider. We carry out intuitive privacy analysis of the proposed protocol system. We consider the security issues that are important protecting patient's privacy.

A. *Attacker Model*

Internal treats from the service provider cannot be eliminated or removed completely in reality. So, our attacker model takes partial untrustworthy service providers into account in which individual employer may try to breach patient privacy. We omit eavesdroppers of user's network traffic as attackers, since secure communication between hosts can be used. We assume that an attacker cannot break cryptographic primitives and does not control the communication network.

In P^3HR database, no quasi-identifiers are stored and it uses patient created secret pseudonym for linking records with their respective patients. The resulting database becomes most likely completely anonymous. Unlike *k*-anonymity or *l*-diversity method, attribute values of a record are not generalized or modified and hence the accuracy of the stored data is preserved. The relationship between a patient and her pseudonym is known only to the patient. A patient let healthcare professionals to access her anonymous health records without revealing her secret pseudonym.

Database Intruders: The database administrator (or an intruder) may get full access on the stored health records. However, since the relationship between the pseudonym in a record and the respective patient is secret and known to the respective patient only, the database administrator cannot find out who is the holder of the pseudonym. Thus, the records are most likely to be completely anonymous to him. This is true for any attacker.

Replay attack: The healthcare professional who has accessed the health records of the patient may try replay attack to access the patient's records until he holds the patient's IC card. However, since the authorization protocol deletes the EAT value from the patient's card and that value is not visible to the healthcare professional, he cannot repeat the access request once the patient's card is taken out from the reader. Ultimately the EAT value changes when the emergency access is reset. So future attempt with possible acquired EAT value does not allow the attacker to access the records.

Non repudiation: Emergency access does not facilitate to take prior permission of the patient at the time of emergency. However, it is very important for life saving. Thus, the privacy awareness must report any access to the patient. Our proposed protocol stores the accessing doctor's identity information into the patient's card during the authorization process. The IC card can protect this information unless someone can know the patient's password and reset's the value. Thus, an emergency access keeps track or proof of the access and it gets non-repudiation property.

V. Discussion

Privacy-aware Patient-controlled Personal Health Record (P^3HR) system is not meant to be an alternative to healthcare centers' usual local health records system. Instead, it is intended to provide a convenient, easy, secure and privacy-preserving way of making patient's personal health history available to any healthcare center at any time according to the patient's desire. We presented the architectural details of P^3HR system in another paper. In this paper, we have considered the privacy awareness in emergency access situations. Intuitive privacy and security analysis shows that the proposed protocol meets the required privacy and security properties for privacy protection from unauthorized entities as well as can share the required personal health records with authorized healthcare professionals when necessary. We also have created a demo version of the application to demonstrate how the devised technology works.

Personal health records of a patient would come from different healthcare organizations where he/she has been treated or diagnosed and different healthcare organizations would have different database structures. Thus, the compatibility between the P^3HR database and external health databases (from where records would be collected) is an important issue. The less number of quasi-identifiers retain in the database and the simpler the database is, the more compatible it would be with other databases. Our observation is that for keeping important health history, PHR databases need not be very complex and few quasi-identifiers might be sufficient. We need to select important quasi-identifiers carefully so that the information loss due to anonymization becomes minimal.

Different patient uses different pseudonyms for the same quasi-identifier. Each time a patient's health information is accessed from the P^{3}HR database, some calculation overhead (to compute the original records with the help of personal pseudonym tables) is incurred. Unless the original records are calculated back, such an anonymous database would contain non-real data (i.e., pseudonyms). Even though such an anonymous database offers very limited usability for data mining, it can provide important health history with privacy protection.

References

[1] L. Røstad, An Initial Model and a Discussion of Access Control in Patient Controlled Health Records, The Third International Conference on Availability, Reliability and Security, pp.935 – 942, Mar. 2008.

[2] M. I. Kim and K. B. Johnson. "Personal health records: Evaluation of functionality and utility." Journal of the American Medical Informatics Association vol. 9(2), pp.171–180, 2002.

[3] Almex Ltd. "Custom health smart card", last accessed on December 15, 2008 from (http://www.smartcardsource.com/health.html)

[4] R. Hillestad, J. Bigelow, A. Bower, F. Girosi, R. Meili, R. Scoville and R. Taylor, "Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs", Health Affairs, vol.24(5), pp.1103-1117, 2005.

[5] V.J.Willey and G.W. Daniel, "Healthcore: An Economic Evaluation of use of a Payer-based Electronic Health Record within an Emergency Department", http://event.on24.com/event/35/62/1/rt/1/images/player_docanchr_5/study.pdf, (2006).

[6] K.D. Mandl, P. Szolovits, and I. S. Kohane. Public standards and patients' control: how to keep electronic medical records accessible but private commentary: Open approaches to electronic patient records commentary: A patient's viewpoint. BMJ, vol. 322(7281), pp.283–287, 2001.

[7] Indivohealth, personally controlled health records, last accessed on October 25, 2008 from http://www.indivohealth.org/

[8] Google, Googlehealth, last accessed on October 25, 2008 from https://www.google.com/health

[9] Microsoft Corporation, HealthVault, last accessed on October 25, 2008 from http://www.healthvault.com/

[10] Md. Nurul Huda, Noboru Sonehara, and Shigeki Yamada: A Privacy Management Architecture for Patient-Controlled Personal Health Record System, Proc. of the International Conference on Network Applications, Protocols and Services 2008 (NetApps2008), University Utara Malaysia , Nov 2008, Paper No.5

[11] E. Ferrari; B. Thuraisingham, Analysis of Information Security Objects Under Attacks and Processed by Methods of Compression, IRM Press, Oct. 2005.

[12] JMC. Brook, "Pseudonymization Methodologies: Personal Liberty vs. the Greater Good", The Last HOPE Conference, New York, Jul.2008.

[13] D.L. Chaum "Untraceable electronic mail, return addresses, and digital pseudonyms", Communications of the ACM, vol. 24(2), pp. 84 – 90, Feb. 1981.

[14] P. Schartner, and M. Schaffer, "Unique User-Generated Digital Pseudonyms", Springer LNCS vol.3685, pp.194-205, Sept. 2005

[15] L. Sweeney "*k*-anonymity: a model for protecting privacy", International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10(5), pp. 557 – 570, 2002.

[16] A.Machanavajjhala, D.Kifer, J.Gehrke and M.Venkitasubramaniam "L-diversity: Privacy beyond k-anonymity", ACM Transactions on Knowledge Discovery from Data (TKDD), vol. 1(1), Article No.3, 2007.

[17] National health Service, NHS Choices homepage, last accessed on October 25, 2008 from http://www.nhs.uk/Pages/homepage.aspx

[18] iHealth Alliance, Interactive Personal health records, last accessed on October 25, 2008 from (http://www.ihealthrecord.org/)

[19] Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC) paper, "Break-Glass – An Approach to Granting Emergency Access to Healthcare Systems," December 2004, last accessed on December 15, 2008 from (http://www.nema.org/medical/spc)

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.6008
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.6008