KEY ISSUES AND FUTURE PERSPECTIVES ON IDENTITY MANAGEMENT IN EHEALTH
A Review

Maria João Campos[1,2] and Pedro Pereira Rodrigues[1,3]
[1]Faculty of Medicine of the University of Porto, Al. Prof. Hernâni Monteiro, 4200-319 Porto, Portugal
[2]Faculty of Sciences of the University of Porto, Rua do Campo Alegre, s/n, 4169-007 Porto, Portugal
[3]LIAAD - INESC Porto, L.A. & CINTESIS
Center for Research in Health Technologies and Information Systems, Porto, Portugal

Keywords: Identity management, eHealth.

Abstract: Identity management represents an essential component for identification, authentication and authorization of patients, professionals, stakeholders and organizations in eHealth, combining information technologies and organizational procedures to provide security and privacy to health information. A literature search was conducted to identify relevant articles which were then grouped into themes according to the main subject. From the selected articles, plus their references, main findings, issues and future perspectives were systematized. A total of 31 articles were obtained, and after selection methodology 13 articles were included and grouped in four different themes: identity pseudonymisation and anonymization for secondary use, privacy preserving identity, identification, authentication and authorization identity in eHealth and identity and standardization. Through references cited in articles, research programs and working areas were also identified. Very few implementations could be found in literature, showing that this problem is even more complex than it seems and future adoption requires further research on new models and architectures. Furthermore, there is the need for a standard methodology for identity attributes interoperability between different stakeholders. Although there is a known large research effort in the context of identity in the information society in general, very few studies and experiences were found in the eHealth context.

1 INTRODUCTION

In the nineties eHealth (Oh, 2005) was related with the transition from paper based to electronic health records. However eHealth has today a broader scope and the emphasis has been changing from the process and the health organization to citizen or patient centred healthcare. Different stakeholders (Slamanig, 2008) play a role in eHealth, information exchange must be established in different contexts, such as between patient, health care professional, different hospitals, external laboratories, health center and pharmacy. In these contexts the patient empowered is needed and there is a strong requirement for an easy access to health information.

Identity management is related with the secure management of identities, the identification process during which an entity may be authenticated in some context. The context for the identification process may be within one organization, or federated across different organizations. It covers the lifecycle of the identities, and respective information, as they are established, modified, suspended, terminated or archived. Entities might be anything that can be uniquely identified, such as persons, organizations or goods (Hildebrand, 2006).

As long as information exchange is needed, data security, safety and the protection of privacy are essentials for eHealth acceptance. Safety and privacy protection assurance are related with the level of security provided by the authentication mechanism used, but also by the registration process preceding them, its respective lifecycle, associated technologies, trust and transparency.

The main goal of this study is to conduct a literature review for the key issues and future perspectives on identity management in the eHealth context.

Campos M. and Pereira Rodrigues P..
KEY ISSUES AND FUTURE PERSPECTIVES ON IDENTITY MANAGEMENT IN EHEALTH - A Review.
DOI: 10.5220/0003124504550458
In *Proceedings of the International Conference on Health Informatics* (HEALTHINF-2011), pages 455-458
ISBN: 978-989-8425-34-8

2 METHODOLOGY

In this section, search query, study selection criteria and study characteristics defined are described.

2.1 Search Strategy and Study Characteristics

A comprehensive literature search was conducted on PubMed and IEEE Xplorer to identify relevant articles published. The keywords that were used include identity, identity management, identity-management and identification, authentication and authorization. These terms were used in conjunction with eHealth, e-Health or electronic health.

2.2 Study Selection

The titles and abstracts of the identified studies were analyzed. Studies that cover identity, but with general reviews and not focused on identity management in context of eHealth were excluded. This exclusion criteria was used because the primary aim of the review was to provide an identification of the main findings, issues and future perspectives on identity management in eHealth context and articles targeting other application areas other than the eHealth context (e.g., information society) were beyond the scope of this review.

For the studies selected to be included in this review, the references cited were also manually examined to identify additional relevant studies and studies were grouped in themes, based on the main area of each study and its main findings.

3 RESULTS

First, general overview result are presented following a thematic analysis with identified themes. Finally, research programs and working groups cited in studies are described.

3.1 General Overview

Following the previously described method, the search queries in Pubmed identified 17 studies and 14 in Xplorer database. Most of the studies included were conducted in Europe (69%) and Australia (15%), and most of them were conducted in the past three years (85%). No studies were found, conducted in United States.

These studies approach identity management from different perspectives and enabled the identification of key themes, based on the main study subject identified as: identity pseudonymisation and anonymization for secondary use, privacy preserving identity, identification, authentication and authorization and identity and standardization. References and citation from other included studies can be included in thematic analysis.

3.2 Thematic Analysis

In this section, thematic analyses from the results of the review are presented, grouped by the themes previously identified.

3.2.1 Pseudonymisation and Anonymisation Identity for Secondary Use

The pseudonymisation and anonymisation for secondary use of electronic health records or personal medical records, is important to ensure the protection of private and personal data, when it leaves the control and protection sphere of the health care, for secondary uses such as clinical or epidemiological and health care research projects, assessment of treatment quality or economic assessments (Iacono, 2007). For these uses, in general the patient identity is not needed, and therefore the data must be anonymised or pseudonymised. Technical approaches for pseudonymisation and anonymization for preserving patient identity privacy are presented, whereas for one-time use of the data the procedure for anonymisation is straightforward, long term data accumulation or the need for re-identification process requires a more sophisticated approach (Pommerening, 2004).

3.2.2 Privacy Preserving Identity

When considering access to eHealth systems and sharing of personal health information in distributed systems within different organizations, security and privacy must be addressed, in particular, compliance with relevant privacy legislation must be established. Some solutions are pointed out, such as federated identity management, that can enable users and service providers to securely and systematically manage identities and user profiles in a single sign on framework that controls access to personal information (Peyton, 2007). However, federated identity management presents a specific privacy threat because it makes intensive use of identity information (Mina, 2008) between different health care providers.

A key component for user privacy is preserving the ability to remain anonymous (Au, 2008). Anonymisation can represent a threat because accountability is important in data security management (Au, 2008).

Privacy-preserving allow different uses of identifiers called pseudonyms in different medical contexts to preserve user privacy. Sensitive medical information can be collected from distributed health record databases in different health organizations and linked together dynamically without revealing the consumer's real identity using concepts like identity management. Anonymity and obfuscation are under well-defined policies with legal-compliance (Au, 2008) and prevents disclosure attacks and statistical analysis (Slamanig, 2008). Sharing medical data on large scale can also expose the patient privacy-related threats, such as massive data aggregation or profiling (Mina, 2008)..

3.2.3 Identity, Authentication and Authorization

Medical data security is an important issue that poses technical, organizational and ethical challenges (Al-Nayadi, 2007). Identity, authentication and authorization level depends on who is getting the access, and different levels are defined for different resources. Attribute certificates, identity certificates, patient consent are important mechanisms to define fine grained rules to grant access.

Some studies (Dagdee, 2009, Hildebrand, 2006) proposed systems that are able to define access control rules using combination of standard, identity and authorization credentials simplifying the specification of access control policy. However, the use of associated attributes with the standard credentials considerably helps in achieving the required fine grained access control. Another important issue that is addressed (Quantin, 2007) is when eHealth systems are used anywhere, through internet access. In order to know that the right person is getting access to the right record anywhere, strict identity check is needed and cryptographic techniques, such as those of electronic signature should be use. This will ensure the authentication of the requests sender and the integrity of the data and also the protection and confidentiality of the access follow up.

3.2.4 Identity Management and Standardization

Several standards are under development for Health Informatics and security domains, such as ISO/TC215 and ISO/IEC-CD24760 with the scope defined for Standardization in the field of information for health, and health information and communications technology (ICT) and identity management respectively. The identity management standard aims to provide a framework for the definition of identity and secure, reliable and private management of identity information. Other ISO committees activities under the group of security techniques (Hildebrand, 2006). Standardization is needed to provide interoperability between different eHealth systems, providing the privacy and security related with identity exchange information and controlling process of observability, linkability, data aggregation and profiling (Hildebrand, 2006).

Significant work has been done on standardization, but many of the results are not known to the user nor has their usability been fully evaluated. Standardization bodies are urging input from the users (Hildebrand, 2006).

3.3 Research Programs and Working Groups

BioHealth and the Liberty Alliance are research programs, focused on identity and standards, promoting awareness, knowledge and understanding of privacy issues and existing and emerging security standards in the area of eHealth. Some of their main results and future perspectives are presented in several articles (Hildebrand, 2006, Peyton, 2007).

In Australia, electronic health implementation (Au, 2008) was promoted, through HealthConnect scheme and more recently through the Australian National e-Health Transition Authority (NETHA, 2007), whose expectation is that through such initiatives this research on consumer-centric identity management will be able to gain acceptance (Au, 2008).

4 DISCUSSION

Research has been made, in eHealth context, in the last three years (11 studies) and based on the literature, research was essentially made in Europe and the main interest was in exploring different architectures and models that can be implemented in the future with identity management in eHealth, based on a patient's centric approach and on federated model in identity management.

Significant evidence has been found highlighting major issues in dealing with identity, especially in the context of eHealth, because of the sensible information, data security and privacy. On the other hand, legal barriers on exchange identities information, makes the need for research new compliance architectural and models. In general, very few studies have been implemented. This is an indicator that identity management in eHealth is much more complex than it seems and that, reliable and trustable, data security and privacy are very difficult to achieve.

Considering the patients and health professionals mobility and that the access should be granted anywhere, several research groups are defining standards to provide interoperability between different eHealth systems. The standards should provide privacy and security related with identity exchange information and the control of key issues such as observability, linkability, data aggregation and profiling. Also, there is no consensus and no standardization methods for anonymisation identification for research propose.

EHealth allows patients to actively participate in the process of health care, improves their awareness and feeling of security, and ultimately leads to their empowerment. Nevertheless, there is no evidence found on the acceptance of patients and health care providers on the use of trustable mechanisms and models on identity management to provide enhanced security and privacy. Attitude and behaviour for patient and health care providers related with identity management in eHealth should be considered for further research.

5 CONCLUSIONS

Identity management is a key component for eHealth. The need for a standard methodology for identity and authentication interoperability between different stakeholders in eHealth was identified. Although a large research effort was found in the context of identity management in the information society, very few studies and experiences were found in the eHealth context. Since eHealth deals with sensible information there is a need for further research work showing evidence that privacy and security are really achieved.

Legal and security issues associated with availability, integrity and confidentiality, related with identity in eHealth, were expected to be found in the literature. However no such themes were found. These are important themes that should be further discussed because they are the main barriers for the implementation of identity management in the context of eHealth.

ACKNOWLEDGEMENTS

The authors acknowledge the help of Luis Antunes for fruitful discussions on this work.

REFERENCES

Al-Nayadi, F., Abawajy, J. 2007. An Authentication Framework For E-Health Systems. *Signal Processing And Information Technology, 2007 Ieee International Symposium On.*

Au, R., Croll, P. 2008. Consumer-Centric And Privacy-Preserving Identity Management For Distributed E-Health Systems. *Hawaii International Conference On System Sciences, Proceedings Of The 41st Annual.*

Dagdee, N., Vijaywargiya, R. 2009. Credencial Based Hybrid Access Control Methodology For Shared Electronic Health Records. *Information Management And Engineering, 2009. Icime '09. International Conference On.*

Hildebrand, C., Pharow, P., Engelbrecht, R., Blobel, B., Savastano, M., Hovsto, A. 2006. Biohealth-The Need For Security And Identity Management Standards In Ehealth. *Stud Health Technol Inform.*

Iacono, L. L. 2007. Multi-Centric Universal Pseudonymisation For Secondary Use Of The Ehr. *Stud Health Technol Inform.*: Pubmed.

Mina, D., Scandariato, R., De Cock, D., Preneel, B., Joosen, W. 2008. Identity In Federated Electronic Healthcare. *Wireless Days, 2008. Wd '08. 1st Ifip.*

Netha. 2007. *"Framework For Analysing, Planning And Implementing Identity Management Within E-Health",* [Online]. [Accessed 8 January 2010].

Oh, H., Rizo, C., Enkin, M., Jadad, A. 2005. What Is Ehealth (3): A Systematic Review Of Published Definitions. *Journal Of Medical Internet Research,* 7 (1).

Peyton, L., Jun, Hu., Chintan, Doshi., Seguin, P. 2007. Addressing Privacy In A Federated Identity Management Network For Ehealth. . *Eighth World Congress On The Management Of Ebusiness, 2007. Wcmeb 2007.* .

Pommerening, K., Reng, M. 2004. Secondary Use Of The Ehr Via Pseudonymisation *Stud Health Technol Inform.* Pubmed.

Quantin, C., Allaert, F. A., Fassa, M., Riandey, B., Avillach, P., Cohen, O. 2007. How To Manage Secure Direct Access Of European Patients To Their Computerized Medical Record And Personal Medical Record. *Stud Health Technol Inform.* Pubmed.

Slamanig, D., Stingl, C. 2008. Privacy Aspects Of Ehealth. *Availability, Reliability And Security. Third International Conference On 2008.*