

Technical and architectural response to national challenges – The Triangle of eHealth Service Provision

Asbjorn HOVSTO ^{a 1} and Peter PHAROW ^b

^a *Portahead, Gjøvik, Norway*

^b *eHealth Competence Center, Regensburg University Hospital, Regensburg, Germany*

Abstract. Due to the strong economic efforts required for developing innovative solutions in new promising markets, such those related to eHealth, the sustainability of investment becomes a key element for large and small companies. Even if it can't guarantee market success, following standards can help guaranteeing long-lasting solutions. Among all innovative sectors, eHealth represents one of the most challenging sectors from the standardization viewpoint as it combines different domains typical of medicine with other issues such as security, safety, ethics or social guidelines. Most likely, this fragmentation of competences is a component of the difficult diffusion of standards which undoubtedly characterizes eHealth and is a justification of the efforts carried out at an international level, in order to involve all its stakeholders. The aim of the present paper is describing how information on applied security and identity management standardization can be provided to users, and how these issues suggest the visualization of eHealth as a triangular domain whose vertexes are represented by security, safety, and related technology and whose area is the domain of the social and ethical requirements. This representation corresponds to the approach followed by the EU "BioHealth" project which aims to increase the stakeholders' knowledge about existing and emerging security and identity management standards in eHealth [1].

Keywords: eHealth, Security, Safety, Ethics, Biometrics, RFID, Standardization

Introduction

The healthcare and welfare domain around the globe, in both developed and developing countries, is turning towards an extended integration of different disciplines. Since high quality healthcare, based on accurate diagnoses and best treatments, requires individuals to share sensitive, personal information with their doctors and other healthcare professionals, issues such as security, safety and privacy

¹ Corresponding Author: Asbjørn Hovstø, Security and Biometrics, represents also ITS Norway, Grenseveien 92, P.O.Box 6086 Etterstad, N-0601 Oslo, Norway. expert@itsnorway.no. Phone: +47 951 48828. <http://itsnorway.no>

are becoming crucial. If patients are not confident that information will be kept confidential or that safety of processes are not completely secure and safe, they will not be forthright and reveal accurate and complete information. On the other hand, if healthcare providers are not confident that the organization responsible for *the healthcare record* will keep it confidential, they will limit what they put in to the record and either of these two considerations is likely to lead to an inferior healthcare [2]. e-health may be described as the central hub of a this vision of medicine combining health telematics, telemedicine, privacy and security. With reference to this last issue, in getting the patient (and citizen) into the center of all processes, a primary role will be played by secure communications and trusted cooperation among the different healthcare providers involved in the patient's care. In the light of an increased mobility of the individuals, especially at the EU level, this "high level" communication can only be met by *adequate national and international networks* of healthcare establishments and health professionals. In this context, the compliance with respective standards shall increase technical (functional) and semantic interoperability among all stakeholders that form both the domains of eHealth and personal Health (pHealth)..

1. Materials and Methods

Advanced concepts of e-health place the citizens in the focus of a net-centric architecture in which the peripheral is represented by cards and tokens that can bear medical data, improve accessibility to information on services and data, or just serve as authentication token. Since they enable a high-level healthcare data and services access and provision, aspects like security, safety, ethics as well as underlying and supporting technologies need to be clearly addressed before establishing a technical solution. The preferred way to deal with the future challenges of modern healthcare requirements shall be a well-balanced combination of mobile personalized security devices and advanced health networks for both information and services provision. The identity management for all principals (persons, systems, applications, devices, components, etc.) is the key for all further security and safety services. Thus, concepts of security, safety, privacy, quality, and ethics play an important role in the framework of advanced health services. Technologies like biometrics, Radio Frequency Identification (RFID) and Near Field Communication (NFC) are able to technically support the legal, political, and social requirements for such advanced healthcare and welfare service provision [3], [4], [5].

2. Security and Safety Requirements

The security requirements in the medical area, technically speaking, are not particularly different from those required in other domains. Apart from a very demanding and dynamic privilege management and access control policy, medical and health applications (like in hospital, diagnostic images, laboratory information systems, General Practitioners office software and many other software solutions) base their security functions' provision on available proper mechanism and algorithms for authentication (identification and verification), identity management, confidentiality, integrity as well as availability and accountability [6], [7].

Additionally, aspects related to mechanical, electrical and electromagnetic safety, and play a crucial role in eHealth because safety of patients overrules virtually any other legislation, both in normal and emergency operations. Any technology applied in healthcare needs to strictly and comprehensively address these security and safety requirements derived, e.g., from respective legislation and ethical rules [5].

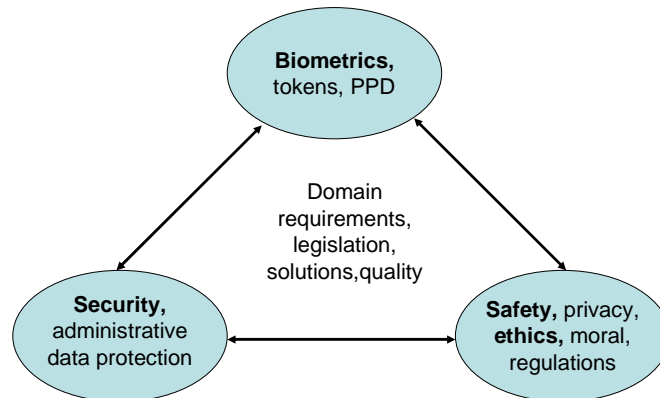


Figure 1. The e-health “Good Practices” Triangle

2.1. Security Requirements towards Advanced Technologies

In Europe and other parts of the globe, security technology is frequently used for enabling trustworthy communication and application security services [6]. With reference to Object Management Group (OMG)’s definition of “principal” [8] a basic security principle reflects a certified binding of a principal to its electronic unique identifier or assigned properties, rights and duties, also called attributes of that principal. Application security services deal with authorization and access control to data and functions. Besides, they also cover accountability of principals, audit track and auditing of these principals and services ensuring integrity, confidentiality of data and functions. Communication security services concern the identification, authentication, and verification of communicating principals. In an end-to-end secure communication environment (object security), these services are used for authentication and control of access rights of principals communicating as well as integrity, authenticity, confidentiality, and accountability including non-repudiation of origin, receipt, and information exchanged. For such security objects, security-aware principals are needed [3], [6].

Integrity and confidentiality of communicated data may also be provided at a system level transparent to the application and to the user following – but not requiring – the user’s awareness for those security measures (channel security). Another important requirement for both communication and application security concerns the availability of information and services. More information regarding the different security categories, services, and underlying mechanisms can be found in [6], [7].

2.2. Safety Requirements towards Advanced Technologies

In the development of advanced technologies particular attention should be paid to safety requirements. With reference to the e-health context a specific interest is represented by some authentication devices such as biometric sensors or RFID.

2.3. Safety Requirements in Identity Management

There are two main sources of concerns for safety in the domain of the biometric authentication. The first one is represented by the possibility of being infected touching the sensor (e.g. hand-geometry or even fingerprint readers). Even if this possibility may be considered equivalent to that arising in touching a door knob or a telephone, it is anyway true that hospitals represent high-risk locations. Hospital-acquired infections (HAIs), also known as healthcare associated infections, encompass almost all clinically evident infections that do not originate from a patient's original admitting diagnosis [9]. Nosocomial infections are caused by viral, bacterial, and fungal pathogens. Therefore also the use of a sensor may result in a potential exposure to risk.

Other concerns may arise from the use of biometric sensors which use the eye as a source of information. Iris recognition systems use LED (Light Emitting diodes) which diffuse near-infrared light (NIR) to improve iris detail with dark irises. Unlike UV, IR does not have the energy to produce photochemical damage but NIR illuminators may pose safety issues since the eye does not respond to NIR and does not protect itself as with visible light by means of pupil contraction, avoidance or blinking.

As it attains safety standards or iris recognition systems, LED Eye Safety Standards apply and therefore the following standards and regulations (for references see the respective organizations' homepages):

- ANSI Z136.1 "Safe Use of Lasers"
- American Conference of Government Industrial Hygienists (ACGIH) 'Threshold Limits Values', 1994
- ICNIRP (1996) laser guidelines for exposure limits (ELs)
- IEC / EN 60825-1
- International Commission on Non-Ionizing Radiation Protection. Guidelines on limits for laser radiation of wavelengths between 180 nm and 1,000 nm. Health Phys. Defined in 71:804–819; 1996
- International Commission on Non-Ionizing Radiation Protection. Revision of guidelines on limits for laser radiation of wavelengths between 400 nm and 1,400 nm. Defined in Health Phys. 2000

While biometrics is used for persons, RFIDs have a primary role in e-health since they improve dramatically the identifications and traceability of materials. Some concerns because of the pollution induced and some documents highlight the necessity of further investigation. Main safety standards for RFID are:

- EN55022 Class A equipment (EN61000-6-3:2001) for emissions
- EN61000-6-2:2001 for industrial immunity
- EN60950:2000 safety standard for Information Technology Equipment

3. Technical Challenges and Solutions for Security and Quality

Healthcare does not allow any kind of compromise in terms of confidentiality, integrity, availability, accountability, authenticity or reliability and therefore require an extra safe data management since compromising the rating of a hospital's IT assets is very likely to have an unfavorable impact, including the risk of a significant financial loss. Consequently, there is an increasing and critical need to protect information and to manage the security of information and communication systems.

While the original motivation for introducing IT security measures has often been security enhancements, appropriate security solutions also offer substantial potential for cost savings and for accomplishing new business opportunities. The ISO/IEC 20000 standard benchmarks the capability of organizations in delivering managed services, measuring service levels and assessing performance. The implementation of ISO/IEC 20000 will reduce operational exposure to risk, meet contractual and tendering requirements, demonstrate service quality and deliver the best possible service. Accordingly it can result in cost savings for users, large or small organizations as well as increased productivity and improved customer service. Regarding software asset management, the implementation of "ISO/IEC 19770-1:2006, Information technology – Software asset management – Part 1: Processes", enables organizations to benchmark their capability in delivering services, measuring service levels and assessing performance. Until now the application of these business processes has been arbitrary, and relatively few organizations have been able to implement a comprehensive software asset management strategy with the potential of massive savings in license costs and maintenance fees.

4. Discussion of Results and Strategies

Although everyone recognizes the importance of sticking to standards in the design of e-health applications, its intrinsic interdisciplinarity represents an evident factor of complexity. Moreover, even if all stakeholders of a project have a sufficient knowledge of the technical and standardization domains, some aspects, such as privacy related or ethical issues are difficult to approach both due to their "vagueness" both because of the different perception at the international level. In the course of the BioHealth project, such aspects have been clearly individuated but, at the same time a certain difficulty has emerged in promoting standards in e-health. Three major issues seem to have priority: (i) make a selection in the domain of stakeholders to find the most appropriate ones for the relevant application, (ii) adopt user-friendly approach, such as multimedia (video, animation, simulation, etc.) to highlight the benefits of standardization, and (iii) propose a centralized approach, at a EU level, to manage the identity management problems concerning technical and ethical issues [4], [5], [6].

5. Conclusion and Outlook

A reliable and secure identification is the basis for all advanced security and safety concepts. This is particularly true for health information systems and applications which require an empowerment of all parties (principals) requiring a secure and trustworthy way of communication and collaboration. Moreover they depend strongly

on common acceptance which, in its turn, is strictly correlated to privacy and ethical issues [9], [10], [11].

Different technologies including biometrics and RFID, allow for guaranteeing high-level security and safety services addressing proper identification of both human beings and goods but diffusion of standards in these fields is still away from a satisfactory level. Projects such as BioHealth, promoting the knowledge about standards, may be extremely useful in supporting e-health applications but, at the same time, they often require a time frame that exceeds the duration of the project.

Acknowledgement

The authors are in debt to the European Commission for supporting and funding the “BioHealth” project within Europe INNOVA Platform Initiative as well as many other partners and organizations (including ISO TC 215, ISO/IEC JTC1/SC 37, CEN TC 251, CEN TC 224, EFMI, ICAO, CEN/ISSS, IEC, ITU, and HL7) for their permanent support and cooperation in all areas of security, safety, and privacy standardization and policies [1].

References

- [1] EU project BioHealth “Security and Identity Management Standards in eHealth including Biometrics - Specific Requirements having an Impact on the European Society and on Standardization”. Scheduled 2006 - 2008. <http://mirc.gsf.de/biohealth/> (last accessed November 15th, 2007)
- [2] HIMSS Privacy and Security Principles. http://www.himss.org/content/files/CPRIToolkit/version6/v6%20pdf/D02_Privacy_and_Security_Principles.pdf (last accessed November 13th, 2007)
- [3] Blobel B, Pharow P (Eds.): Advanced Health Telematics and Telemedicine. The Magdeburg Expert Summit Textbook, pp. 21-28. Series “Studies in Health Technology and Informatics” Vol. 96. IOS Press, Amsterdam 2003
- [4] Kluge EHW: Medical Narratives and Patient Analogs: The Ethical Implications of Electronic Patient Records. *Methods of Information in Medicine* 1999 38 4: 253-259.
- [5] Ball, MJ, Douglas JV: Redefining and Improving Patient Safety. *Methods of Information in Medicine* 2002 41 4: 271-276.
- [6] Blobel B: Analysis, Design and Implementation of Secure and Interoperable Distributed Health Information Systems. Series “Studies in Health Technology and Informatics” Vol. 89. IOS Press, Amsterdam 2002.
- [7] Pharow P, Blobel B: Security Infrastructure Requirements for Electronic Health Cards Communication. In: Engelbrecht R., Geissbuhler A. (Eds.): Connecting Medical Informatics and Bio-Informatics. Proceedings of MIE 2005. Series “Studies in Health Technology and Informatics” Vol. 116. IOS Press, Amsterdam 2005.
- [8] OMG definition: A principal is an actor in the health systems (including its informational support) such as persons, organizations, systems, devices, applications, components or even single objects. <http://www.omg.org> (last accessed November 16th, 2007)
- [9] Report on Hospital Acquired Infections and its Consequences for Patient Safety. <http://www.emedicine.com/ped/topic1619.htm> (last accessed November 13th, 2007)
- [10] Pharow P, Blobel B, Hildebrand C: The Role of Patient Health Cards in an Integrated eHealth Environment. Submitted to STC 2006: Integrating biomedical information - “From e-Cell to e-Patient”. Timisoara, Romania, 2006.
- [11] Engel K, Kuziela H, Blobel B, Pharow P: Security Services for the HemaCAM Project. In: Engelbrecht R, Geissbuhler A (Eds.): Connecting Medical Informatics and Bio-Informatics. Proceedings of MIE 2005. Series “Studies in Health Technology and Informatics” Vol. 116. IOS Press, Amsterdam, 2005.