Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 64 (2015) 1124 – 1129

Procedia Computer Science

Conference on ENTERprise Information Systems / International Conference on Project MANagement / Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2015 October 7-9, 2015

A standardized SOA based solution to guarantee the secure access to EHR

Giorgia Gazzarata[a], Roberta Gazzarata[a, b], Mauro Giacomini[a, b, c]*

[a]*Department of Informatics, Bioengineering, Robotics and System Engineering (DIBRIS), University of Genoa, Via Opera Pia 13, Genoa 16145, Italy*

[b]*Healthropy s.r.l., Corso Italia 15/6, Savona 17100, Italy*

Abstract

Continued advances in science and technology and general improvements in environmental and social conditions is extending the population's life expectancy with the consequence that a person can undergo many episodes of healthcare during lifetime. In this context, the Electronic Health Record (EHR) represents a fundamental tool to support treatment continuity, education and research. The economic restrictions in healthcare and the need to increase efficiency in term of cost/effectiveness ration could lead institutional organizations to choose cloud solutions to host the EHR. In this paper, a cloud infrastructure architecture, focus on the EHR and based on SOA (Service Oriented Architecture) paradigm, which is able both to completely support technical, semantic and process interoperability, and to guarantee security, is proposed. In order to achieve this goal, the indications and the standards proposed by Healthcare Services Specification Project (HSSP) was adopted. Different situations can be managed by the proposed architecture and are described: the user access to an encrypted resource in EHR, the availability of EHR content for external Decision Support Systems, the update of EHR content, the management of semantic of clinical data exchanged among distributed healthcare organizations. Finally, the authors propose a discussion on the proposed solution.

Peer-review under responsibility of SciKA - Association for Promotion and Dissemination of Scientific Knowledge

Keywords: auditability, access control, interoperability, secure use of cloud for clinical data;

* Corresponding author. Tel.: +39-010-353-6546; fax: +39-010-353-2154.
E-mail address: mauro.giacomini@dibris.unige.it

Peer-review under responsibility of SciKA - Association for Promotion and Dissemination of Scientific Knowledge
doi:10.1016/j.procs.2015.08.582

1. Introduction

Continued advances in science and technology and general improvements in environmental and social conditions have increased life expectancy around the world[1]. These demographic and social trends have the consequence that a person can undergo many episodes of healthcare during lifetime. In order to support physicians to correctly and efficiently treat patients, it is fundamental to design solutions that allows having a complete and precise knowledge of patient's clinical history, especially in case of chronic diseases or acute events[2]. The concept of Electronic Health Record (EHR) was introduced exactly to support these needs. In fact, the EHR represents a digital storage for healthcare information related to a person's lifetime with the goal of supporting treatment continuity, education and research, whilst always guaranteeing privacy protection[3]. Although this definition was introduced already in 1998, only in recent few years the Healthcare Ministries of developed countries, interested in the potential benefit provided by the EHR to modernize the healthcare field and improve its quality, security and efficiency, have planed the creation of national EHR systems[4]. One of the causes of this delay was the absence of both Information and Communication Technologies (ICT) infrastructure and standards that was able to support the interoperability needed to design an appropriate architectural context in which the EHR could be easily accessed by all actors that are involved in patient's treatment. An important aspect to consider is that the collaboration with the physicians in this design is fundamental for the effective success of this application[5] in order to prevent the failure that the National Programme for IT (NPfIT) obtained in UK precisely for clinicians' reluctance to accept the solution[6]. The Service Oriented Architecture (SOA) paradigm represents a suitable approach in this scenario. It was successfully adopted in many solutions to provide an infrastructure to support the communication among several agents within e-health solutions[7,8]. The diffusion of SOA as was due to his feasibility, which promote the easy alignment and integration of new and existing information systems within a cohesive architecture[9]. For this reason, SOA is appropriate for the healthcare context in which the reuse of application and information system is an important evaluation criterion considered by healthcare organizations[7]. Finally, to allow the EHR to be completely useful, it is fundamental to consider data policy access and security too[10]. The economic restrictions in healthcare and the need to increase efficiency in term of cost/effectiveness ration lead to choose cloud solutions instead of remove servers, which now are inefficiently managed, from institutional regional organizations responsible for EHR hosting[11]. In addition, cloud allows to access more easier to information from different point in the same time, aspect which is very interesting in this context, especially in case of emergency situations[12]. However, this propensity is braked by a feeling of suspect of Ethics Committee, which represented the patient's right to data privacy. This common idea is not correct because actually cloud providers adopt data protection protocols, which are studied by ICT experts, that are more efficient than the one used by the these local organizations[13]. Moreover, it is known that public cloud is honest-but-curious and therefore it is tempted to peek into data content stored in itself for different aims (e.g. unauthorized use in clinical trials, health assessment for insurance purposes, employees hiring, etc.). This aspect is unacceptable in healthcare contest, therefore a possible solution to this issue is combine public cloud with private one. In this approach, the private cloud play the role of data processing and cryptography, while the public cloud is responsible for encrypted data storage, which cannot be understood even if peeked[14]. In this paper, the authors propose a hybrid cloud infrastructure architecture, focus on the EHR, that is able, on one hand, to completely support interoperability, and on the other, to guarantee security in terms of access control, auditability and clinical and administrative data cryptography.

2. Methods

The SOA approach was adopted as paradigm to design the overall solution therefore SOAP (Simple Object Access Protocol) messages were used as vehicle to exchange clinical and administrative data mapped through standardized object as HL7 (Health Level Seven) V3 (Version 3) CDA R2 (Clinical Document Architecture Release 2). The SOA paradigm combined with the use of standardized messages is not enough to guarantee an effective interoperability[15]. In fact, these solutions allow supporting technical and semantic interoperability but not process interoperability, which is fundamental in distributed solutions as the ones in the healthcare context[16]. The Healthcare Services Specification Project (HSSP) was formed in 2005 by the HL7 International and the Object Management Group (OMG) exactly to define health industry SOA standards that promote effective technical, sematic and process interoperability between applications and distributed and heterogeneous devices, which belong to independent socio-health system

organizations. In particular, the main HSSP objective is to use the SOA approach to provide and guarantee an effective interoperability between applications, and distributed and heterogeneous devices, which belong to independent socio-health system organizations. The aim of every HSSP project is the standardization of a specific service, which is related to a functional socio-health domain, as a generic service. The intention is to standardize service interfaces that is functions and protocols, which allow application and technical communication, in order to invoke, accept or reject and report the performance of these functions. The HSSP characterized the SOA services into three clear categories, which are: (1) *Technical/Infrastructure Services*, which involve capabilities like proxy service, service instance location, protocol/message routing access and security control, event logging, notification, and exception handling, etc, (2) *Business Services***,** which describe those capabilities that support business competences or processes. Some examples are terminology, payroll, accounting, human resource management and demographics, (3) *Healthcare-Unique Services***,** which call-out service capabilities that are either unique to healthcare, or for which healthcare has unique requirements. For instance, both record management, clinical decision support and order management appear here[15]. For the design of the cloud architecture proposed in this paper, services from all these categories were considered. In particular, were included: Health Access and Security Control Services (HASCS) and Proxy Service from Technical/Infrastructure Services category, Health Terminology Services (HTS) and Health Identity Services (HIS) from the Business Services category, Health Record Management Services (HRMS) and Health Decision Support Services (HDSS) from the Healthcare-Unique Services category. The interfaces of each mentioned services are compliant with specific HSSP standards. Every HSSP product derives from a complex standardization process called HSSP Service Specification Framework (SSF) formed by several steps. The results of the first three steps is the HL7 Service Functional Model (SFM), which provides a service interface specification at a functional level, while the last four steps create the OMG Service Technical Model (STM), which specifies the technical requirements of the service[15]. HTS are standardized services to manage clinic and health codifications and terminologies and their interfaces are defined by Common Terminology Services Release 2 (CTS2) standard. The CTS2 standard provides a consistent specification to develop service interfaces to manage, search and access terminology content, either locally or across a federation of terminology service nodes, independent of the terminology content and underlying technological stack[17]. HIS are standardized services to define, update and generally manage identities and their interfaces are defined by Identification and Cross-Reference Service (IXS) Release 1 standard. The IXS standard provides a set of service interfaces to uniquely identify and index various kinds of entities (patients, providers, organizations, systems and devises) both within and across health organizations[18]. HRMS are standardized services to manage patients' profiles and clinical history and the interfaces are defined by the Retrieve, Locate and Update Services (RLUS) Release 1 standard. The RLUS standard provides a set of interfaces through which information systems can access and manage information within and between healthcare organizations[19]. HDSS are standardized services to research, query and execute modules to help in making decisions and their interfaces are defined by Clinical Decision Support Services (CDSS) Release 1 standard. The CDSS standard provides interface specifications and technical requirements that are needed for a standardized approach for leveraging machine-executable medical knowledge in an application-independent manner[20]. Finally, HASCS are standardized services that manage security in terms of access control and auditability whose interfaces are compliant with the Privacy, Access and Security Services (PASS) Release 1. The PASS standard aims to define a suite of interfaces necessary to guarantee security requirements, such as privacy, control and manage access to clinical data, consensus and identity management[21]. At the present, the PASS is formed by two parts, which are the PASS Access Control and the PASS Audit Control. The Access Control is responsible of providing access to clinical and administrative data only to authorized users. Audit Control plays the role of recording accesses to and operations on data performed within the system. Both Access and Audit Control are at the first steps of HSSP SSF. In detail, the SFM for the Access Control part represents an HL7 Draft Standard for Trial Use (DSTU)[21], while for the Audit Control HL7 is still working to produce a DSTU[22].

3. Results

Figure 1 shows the hybrid cloud architecture compliant to indications and standards produced by HSSP that can be adopted to allow the EHR to be easily accessed by all actors that are involved in patient's treatment. In particular, the EHR is hosted in a public cloud and its content is encrypted to prevent the honest-but-curious provider to interpret patient's clinical and administrative data (yellow shape). All the services mentioned above, which have their specific

role in the information exchange between the EHR and external actors (e.g. Hospital, Patient's home, Laboratory, Decision Support System, General Practitioner, Pharmacy, Research Centers, etc…) are hosted in different private clouds (light blue shapes).

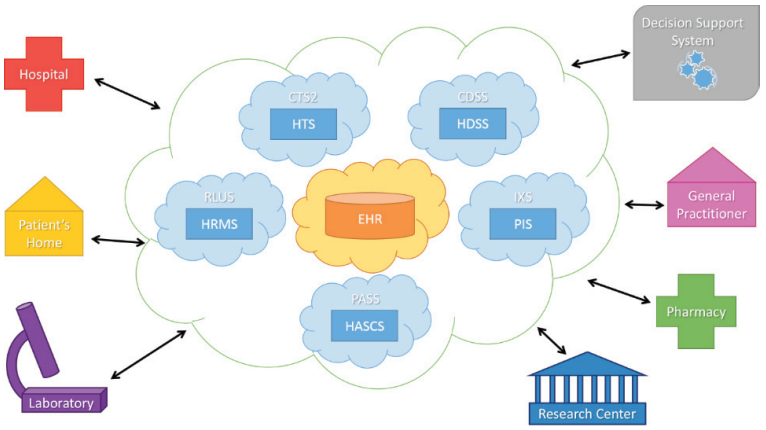

Fig. 1. The proposed architecture.

A simplified diagram, which represents the principal interactions that occur among external actors, the proposed cloud standardized service and the EHR to have access to a specific patient's resource, is presented in Figure 2. To support this situation, the HRMS, whose interfaces are compliant to RLUS standard, provides the *get resource* operation, which is called by the external actor. The Proxy Service intercepts this request and interacts with the HASCS, whose interfaces are compliant with the PASS. In particular, the Proxy Service communicates with the Access Control Service (ACS). An important aspect that the authors consider in the design of the architecture was that a person during lifetime might have different episodes of care provided by several healthcare organizations, many of whom assign and maintain the patient's identifier autonomously. In this context, each organization or even department often assigns its own ID, which uniquely identifies the patient and the medical staff for its own purposes, with the result that these ID values are meaningless outside that system or organization. In order to manage all the identifiers, the authors also introduced the HIS, whose interfaces are compliant to the IXS standard. The Health Identity Services provide query operations, given an identifier, to retrieve the list of all other IDs, which are linked to it. The ACS asks to the HIS two lists of identifiers: the first one provides all identifiers that are linked with the ID of the user which requested the resource, while the second one contains all IDs that are used to identify the specific patient whose information was requested by the user. The Access Control Service matches these lists with the policy, which it manages, to check if the actor is authorized to access the required information. If so, the ACS performs the *get resource request* of Health Record Management Services, which interacts with the EHR and provides the resource mapped through the specific standardized object indicated in the request (e.g. CDA R2). It is important to highlight that the HRMS is responsible of decryption of clinical content, which is stored encrypted in the public cloud that hosts the EHR. Before returning this object to the user, the ACS submits a request to the Audit Service to record the user action. The importance of this last step will be explained below in this section. The proposed architecture allows to support other different workflows, similar to the one shown in Figure 2, that are typical of healthcare distributed environment. A first example is the possibility to provide access to EHR content to external Decision Support Systems and to the international medical community, in order to improve the relevant shared data, which can be processed to provide patient-specific assessments or recommendations. In this case, the workflow is different from the one described above only for the participation of the HSDD instead of Health Record Management Services. In fact, the security aspects are managed in the same manner by the HASCS, while the encrypted information stored in EHR is decrypted and then supplied by the Health Decision Support Services through interfaces, compliant with CDSS standard, suitable for the specific purpose.

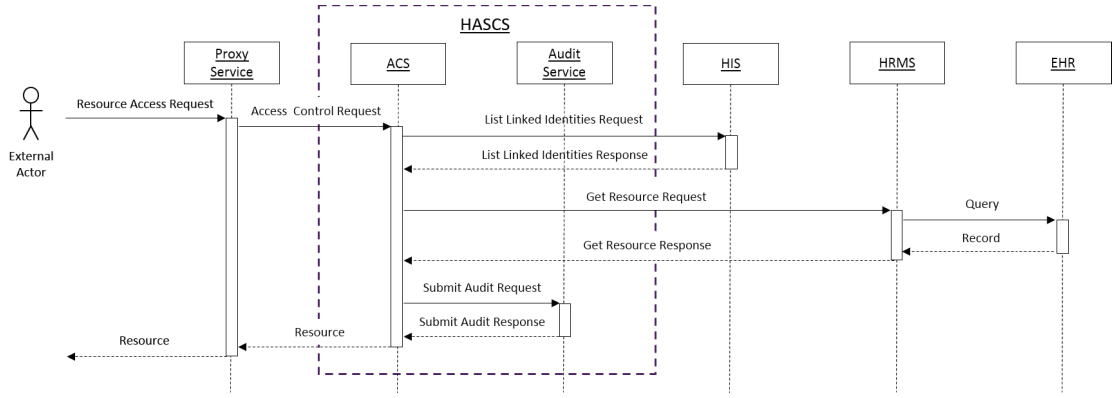

Fig. 2. Interactions diagram to access an EHR resource

Another example is the update of the EHR content, which occurs every time a new resource, related to the patient, is produced from one of the external actors. In this case, the services that participate in the workflow are the same that are reported in Figure 2, but there are two differences: (1) the request performed by the user, and therefore the one that the ACS makes to the HRMS, is no more to get but to put (*put request*) a resource and, consequently, (2) the policy managed by the Access Control Service is no more the one related to read permission, but to write permission. Obviously, the HRMS is responsible for the information encryption before the storage in the EHR. An important aspect, which the authors took into account to provide the architecture to guaranty integrity and consistency in semantic of the clinical data exchanged among distributed healthcare organizations, was the management of terminologies. When a user produces a resource often adopts a local terminology to indicate the semantic of the analytical data. This occurs for example in Italy, as the national effort to provide a standardized nomenclature was motivated by exclusively economic purposes. In fact, it aimed to quantify the amount of refund of outpatient specialist health services and to define the essential levels of assistance founded by the Italian national healthcare system. In addition, this nomenclature was produced in 1999 and it was excluded from the rapid evolution of clinical care world. These limits led to the creation of many different local terminologies, which represent an obstacle to achieving semantic interoperability. For these reasons, the Health Terminology Services were also included in the architecture design in order to permit the sharing of information semantics. HTS, whose interfaces are compliant with the CTS2 standard, provide functionalities (1) to search and query structured terminological content, (2) to maintain local and standardized (LOINC, SNOMED, ICD) terminologies and (3) to map a concept from one terminology to another. Unlike the access of EHR content that has to be controlled both to get and to put a resource, the access to terminology content, managed by HTS, must be authorized only when maintenance capabilities are called. In fact, to promote semantic interoperability, it is fundamental that the terminology content would be available to all actors who need it. In the same time, exactly for the importance of this content, it is required that only authorized users can maintain it. The proposed solution, using the same mechanism described above is able to manage the situation too.

4. Discussion and Conclusion

The proposed infrastructure architecture allows, on one hand, to support technical, semantic and process interoperability and, on the other hand, to assure security in terms of access control, auditability, clinical and administrative data cryptography, integrity and consistency in semantic of the clinical data exchanged. One of the advantage of adopting SOA paradigm combined with the indication of HSSP is certainly its flexibility that allows the system to be future proof, adding and integrating new functionalities to an existing solution. This feature permits the reuse of software, which was financed by previous investments, a fundamental element to be approved by healthcare organizations[15]. In addition, the overall solution was projected in close collaboration with the medical staff in order to

satisfy all its requirements, a crucial point to be accepted by the final users[5,6]. The authors' experience received through the collaboration with clinicians, technicians and patients teaches that one of the most required features is the transparency to the final user[23]. All actors would approve a solution only if it does not necessitate a serious change in their workflow and it consequently produces an important improvement in patient care or a consistent decrease of human errors or time consumption. For example, the insertion of the Health Decision Support Services within the architecture was prompted by clinicians' request to provide data to external Decision Support Systems. The Access Control Service plays an important role in this request because it is able to interact with external policy management system, aspect that is fundamental for the adoption of this solution. Auditability, which consists in recording the external users' actions, is a key aspect to guarantee patient's right to data privacy. In addition, it is a relevant point to defend physicians. In fact, on one hand they cannot deny to have accessed to one resource, and on the other hand, they cannot be falsely accused in case of good behavior. This allow the medical staff to serenely work and to freely manage emergency situations too. The authors restate that the PASS standard is still in development; the considerations and the situations described in Results section are based on the SFM that is only available for the Access Control part. In this documentation, HL7 deals with particular situations such as when a physician forgets the password. In this case, a trusted authority (e.g. another physicians) can certificate the identity of the physician until the system administrator resets the password, important aspect in case of emergency situations.

References

1. Bensink ME, Hailey D, Wootton R. The evidence base for home telehealth. In: *Home Telehealth: Connecting Care Within the Community*. The Royal Society of Medicine Press; 2006:53-62.
2. Yoediono Z, Snyderman R. Proposal for a new health record to support personalized, predictive, preventative and participatory medicine. 2008.
3. Iakovidis I. Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe. *Int J Med Inform*. 1998;52(1):105-115.
4. Black AD, Car J, Pagliari C, et al. The impact of eHealth on the quality and safety of health care: a systematic overview. *PLoS Med*. 2011;8(1):e1000387.
5. Moeckli J, Cram P, Cunningham C, Reisinger HS. Staff acceptance of a telemedicine intensive care unit program: A qualitative study. *J Crit Care*. 2013;28(6):890-901.
6. Fernando S, Choudrie J, Lycett M, de Cesare S. Hidden assumptions and their influence on clinicians' acceptance of new IT systems in the NHS. *Inf Syst Front*. 2012;14(2):279-299.
7. Gazzarata R, Vergari F, Salmon Cinotti T, Giacomini M. A standardized SOA for clinical data interchange in a cardiac telemonitoring environment. *IEEE J Biomed Heal Inf*. 2014;18(6):1764-1774.
8. Chang F-C. A Framework for Prototyping Telecare Applications. 2014.
9. Vasilescu E, Mun SK. Service oriented architecture (SOA) implications for large scale distributed health care enterprises. In: *Distributed Diagnosis and Home Healthcare, 2006. D2H2. 1st Transdisciplinary Conference on*. IEEE; 2006:91-94.
10. Blobel B. Authorisation and access control for electronic health record systems. *Int J Med Inform*. 2004;73(3):251-257.
11. Chen Y-Y, Lu J-C, Jan J-K. A secure EHR system based on hybrid clouds. *J Med Syst*. 2012;36(5):3375-3384.
12. Bahga A, Madisetti VK. A cloud-based approach for interoperable electronic health records (EHRs). *Biomed Heal Informatics, IEEE J*. 2013;17(5):894-906.
13. Wang C, Wang Q, Ren K, Lou W. Privacy-preserving public auditing for data storage security in cloud computing. In: *INFOCOM, 2010 Proceedings IEEE*. Ieee; 2010:1-9.
14. Tong Y, Sun J, Chow SSM, Li P. Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability. *Biomed Heal Informatics, IEEE J*. 2014;18(2):419-429.
15. Kawamoto K, Honey A, Rubin K. The HL7-OMG Healthcare Services Specification Project: motivation, methodology, and deliverables for enabling a semantically interoperable service-oriented architecture for healthcare. *J Am Med Informatics Assoc*. 2009;16(6):874-881.
16. Gibbons P, Arzt N, Burke-Beebe S, et al. Coming to terms: Scoping interoperability for health care. 2007.
17. Hamm R, Estelrich A, Canu N, Oemig F, Nachimuthu S. *HL7 Common Terminology Services, Release 2: Service Functional Model Specification, Normative Release*.; 2013. Available at: https://www.dropbox.com/s/4kt2wkibl44ynnc/CTS2N_SFM_Jan16th.doc?m.
18. Gilbert P, Honey A, Kirnak A, Lotti S, Ries D, Teichrow G. *HL7 Version 3 Standard: Identification and Cross-Reference Service (IXS) Release 1*.; 2013.
19. Lotti S, Koisch J, Honey AP, Robinson S, Kawamoto K. *Service Functional Model Specification Retrieve, Locate and Update Service (RLUS), Release 1*.; 2012. Available at: http://hssp-rlus-normative.wikispaces.com/file/view/RLUS_SFM_R1-Normative.pdf/415574604/RLUS_SFM_R1-Normative.pdf.
20. Fiol G Del, Jenders R, Kawamoto K, Strasberg H. *HL7 Version 3 Standard: Decision Support Service (DSS), Release 1*.; 2011.
21. HL7. *HL7 Version 3 Standard: Privacy, Access and Security Services (PASS) – Access Control, DSTU Release 1*.; 2012.
22. Project Summary for Privacy, Access and Security Services (PASS) Alpha Project. Available at: http://www.hl7.org/special/Committees/projman/searchableProjectIndex.cfm?action=edit&ProjectNumber=200.
23. Giannini B, Gazzarata R, Orcamo P, et al. IANUA: a regional project for the determination of costs in HIV-infected patients. *Stud Health Technol Inform*. 2014;210:241-245.