AUTHORIZATION IN CLOUD E-RADIOLOGY SERVICES

Vassiliki Koufi, Flora Malamateniou and George Vassilacopoulos
Department of Digital Systems, University of Piraeus, 80, Karaoli & Dimitriou Str., Piraeus, 18534, Greece

Keywords: Cloud Computing, Personal Health Record, eRadiology, Healthcare process, Authorization.

Abstract: The confidentiality of healthcare information is extremely important in any healthcare system. This paper is concerned with the development of suitable authorization and access control framework for eRadiology seen as a cloud computing service offered to healthcare professionals and patients alike. While eRadiology is expected to improve many aspects of healthcare, these high expectations will be achieved only if provider organizations pay continuing attention to the features that would most improve patients' safety and health and select systems that have such appropriate features, security being among the most prominent ones. In particular, although the eRadiology workflow varies with the context, giving rise to specific ordering of task executions, it is authorization that determines who can execute the various workflow tasks and what information can be accessed during task executions. The main objective of this paper is to embed context-aware access control into eRadiology workflows, operating in conjunction with a personal healthcare record (PHR) system which has been implemented in a cloud computing infrastructure. The proposed model enables authorization to be based not only on static rules and roles but also to be influenced by the workflow execution context ensuring precise and tight access control. The resultant security system has been incorporated into a prototype eRadiology workflow to enable authorized access to patient information when and where needed.

1 INTRODUCTION

Healthcare providers are increasingly considering migrating to cloud computing in order to exploit its economic, technical, architectural and ecological benefits (Andriole and Khorasani, 2010; Rosenthal et. al, 2010). Cloud computing is an on-demand service model for IT provision, often based on virtualization and distributed computing technologies; it refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. The data center hardware and software is what we will call a Cloud. Thus, cloud computing may be divided into Software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as service (IaaS) (Shimrat, 2009; van der Burg and Dolstra, 2009). Clouds may also be divided into public, which are available publicly (i.e. any organization may subscribe), private, which are services built according to cloud computing principles, but accessible only within a private network and partner, which are cloud services offered by a provider to a limited and well-defined number of parties.

While cloud computing may seem like network computing, a wide expanse of sky separates the two. Networking involves a single entity and its servers. Cloud computing encompasses multiple organizations and their servers connected via the Internet to build a more expensive network that can facilitate potentially universal accessibility. The concept has significant implications for medical imaging and healthcare in general. Cloud computing enables wider sharing (sending and receiving), storage, access and manipulation of data, which can be achieved in a cost-effective, secure and user-friendly fashion (Buyya, Yeo, Venugopal, Broberg, and Brandic, 2009; Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, et.al., 2009). Companies have been offering cloud-based services such as archiving and off-site backup for years. The off-site Picture Archiving and Communication Systems (PACS) archives that many firms offer are one example. A new wrinkle unveiled in 2009 was using cloud-based services to move healthcare information between organizations – an approach to meeting the interoperability objective. Hence, cloud computing

Koufi V., Malamateniou F. and Vassilacopoulos G..
AUTHORIZATION IN CLOUD E-RADIOLOGY SERVICES.
DOI: 10.5220/0003144402730279
In *Proceedings of the International Conference on Knowledge Management and Information Sharing* (KMIS-2010), pages 273-279
ISBN: 978-989-8425-30-0

technology is changing the rules by enabling transfer of medical images and associated information as easily as sending an e-mail (Harvey, 2010).

Given the cloud computing benefits, a Personal Healthcare Record (PHR) architecture based on a combination of the above categories may be used to allow authorized access to patient information at the point of care, anytime. Moreover, cloud PHR architectures can be used to incorporate, through loosely coupling interfaces, crucial healthcare delivery applications, such as eRadiology, requiring little or no manual data entry of patient information (Andriole and Khorasani, 2010). Usually, eRadiology provides teleradiology services to hospitals, imaging centers and physician group practices by using high speed, secure internet connections, instant messaging and advanced Radiology Information System (RIS) and PACS (Benjamin, Aradia, Shreibera, 2010; Telemedicine Information Exchange – TIE Europe, 2005). This technology also allows referring physicians with electronic access to their patient's images and reports via a secure web viewer on the internet. eRadiology also has the expertise to offer assistance with the selection and acquisition of imaging equipment.

The view of an eRadiology system as a cloud computing application that interfaces with a PHR implies that eRadiology is seen as a comprehensive web-based application that streamlines and automates the physician's medical order processes by enabling the electronic transmission of radiological orders from physicians to medical centers and, also, that allows physicians to check patient history and best practice protocols and much more to ensure that the radiological procedures requested is the safest and most effective choice for the patient (Ash, Berg and Coiera, 2004; Terry, 2008; Steele and Lo, 2009). Besides, an eRadiology system can be used to facilitate and enhance communication and coordination between referring physicians and radiologists (Reid, 2010).

One important consideration in developing an eRadiology system as a cloud application is security since security is a priority for many cloud customers (i.e. healthcare organizations) and, on several occasions healthcare organizations will make buying choices on the basis of the reputation for confidentiality (Bruening and Treacy, 2009; Pearson, 2009; U.S. Department of Health and Human Services, 2004). For example, patients need assurances that radiological order or response data will not be used to harm them—for example, through disclosure to a prospective employer. Thus, there is need for adhering to appropriate privacy and security rules to provide the necessary protections and, to this end, audit trails and role-based access controls are strongly recommended (Cavoukian, 2008; IBM Corporation, 2009; Muttig and Burton, 2009).

This paper focuses on a context-aware access control mechanism incorporated into a prototype eRadiology application (NefeliRadiology) which is based on a prototype healthcare portal, called NefeliPortal, which automates the physician radiological request process while it enables access to a cloud PHR. The proposed access control mechanism incorporates the advantages of role-based access control (RBAC) and yet provides the flexibility for adjusting role permissions on individual objects according to context. Thus, at run time contextual information is collected to adapt user permissions to the minimum required for completing a job. Relevant access control policies are enforced at both web service and BPEL task levels.

2 MOTIVATING SCENARIO

To illustrate the main principles of the security architecture incorporated into the NefeliPortal, consider a healthcare process scenario concerned with radiological medical orders (e-radiology). Suppose a healthcare delivery situation where a patient's physician wishes to issue a radiological request for one of his/her patients. The request is sent to the radiology department of an appropriate medical center which schedules the radiological procedure requested and sends a message to the requesting physician notifying him/her on the date and time scheduled. After performing the radiological procedure requested, the radiologist assesses the relevant part of the patient record and writes a radiological report, incorporating both the radiological images and the associated assessment, which is sent to the referring physician.

This scenario shows an example of how a cloud eRadiology service may work: A physician uses an eRadiology application which is interfaced to a PHR stored in a data center, reads the summary record of his/her current patient and selects one or more radiological procedures to be performed on a patient based on an assessment of patients condition. Upon selection of a radiological procedure by the physician, the eRadiology application performs validation checks (e.g. with regard to best practice protocols) to either clear the radiology order or

return notice information to physician. Then, the physician sends the radiological request to the data center where the whole eRadiology activity is captured. Finally, the patient books an appointment with a medical center of his/her own choice for performing the radiological procedures requested by his/her physician. After performing the radiological procedures requested, the radiological report (incorporating both medical images and text) is stored into the patient's PHR which is situated in the data center which is based on a cloud infrastructure while providing relevant access to the referring physician.

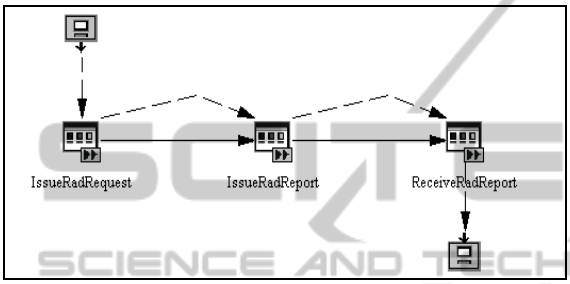

Figure 1: A high level model of an eRadiology process.

The benefits accrued from the implementation of an eRadiology system are manifold: For example, the service puts eligibility and insurance information at the physician's fingertips at the time of radiological order. This enables physicians to select the most effective radiological procedures for the case in hand that are covered by the patient's insurance (Metfessel, 2007; Information Technology in Healthcare, 2004). It also informs physicians of lower cost alternatives. In addition, physicians can access a timely and clinically sound view of a patient's history stored in patient's PHR at the point of care. This decreases the risk of preventable medical errors (Metfessel, 2007; Kaelber, Shah, Vincent, Pan, Hook, Johnson, et.al., 2008). Also, radiological request routing replaces old, error-prone approaches to sending new radiological requests with the secure computer-to-computer exchange of radiological requests between physicians and medical centers. Routing new radiological requests electronically reduces the risk of radiological requests associated with poor handwriting, illegible faxes and manual data entry. Using radiological request routing to process radiological renewals (radio-therapeutic services), saves physician time and money by dramatically reducing the number of phone calls and faxes typically associated with the renewing authorization process (Collin, Reeves, Hendy, Fulop, Hutchings and Priedane, 2008; Bell, Cretin, Merken and Landman, 2004). Figure 1 shows a high-level view of the eRadiology process using the IBM WebSphere Workflow build-time tool (IBM Corporation, 2005). In this process two healthcare providers are involved: the referring physician and the radiologist.

From a role-based workflow authorization perspective, the business process of Figure 1 surfaces several requirements with regard to task execution and associated data accesses. These requirements include the following:

- **Data Content -** Some role holders should be allowed to exercise a set of permissions on certain data objects only. For example, during the execution of the "IssueRadRequest" task, a physician is allowed to read patient records and issue (write, edit and send) radiological requests only for his/her patients.
- **Permission Propagation -** Some role holders should receive additional permissions on certain data objects in order to effectively execute a task but these permissions should be revoked upon successful execution of the task. For example, for an effective execution of the "IssueRadReport" task with regard to a patient, a physician should receive the permission to read the patient's record but he/she should not be allowed to retain this permission after successful task execution. Also, on patient's appointment with a medical center for performing radiological procedures, the attending radiologists are granted the authorization to read patient records.
- **Restricted Task Execution -** In certain circumstances the candidates for a task execution should be dynamically determined and be either a sub-group of the authorized users or only one, specific authorized user. For example, when a radiological request issued by a physician is stored in the data center and relevant access rights are routed only to the appropriate group of medical centers (e.g. within a health district).

Table 1 shows an extract of workflow authorization requirements regarding task execution and related data access privileges assigned to the "referring physician" and "radiologist" roles, respectively. Similar requirements exist in many healthcare workflow application fields where request-service situations occur (Poulymenopoulou, Malamateniou and Vassilacopoulos, 2005).

These authorization requirements suggest that certain data access permissions of the eRadiology workflow participants depend on the eRadiology

process execution context. In particular, contextual information available at access time, like location or user/patient relationship, can influence the authorization decision that allows a user to perform a task and access associated data objects. This enables a more flexible and precise authorization policy specification that incorporates the advantages of having broad, role-based permissions across workflow tasks and data object types, like RBAC, yet enhanced with the ability to simultaneously support the following features: (a) predicate-based access control, limiting user access to specific data objects, (b) a permission propagation function from one role holder to another in certain circumstances, and (c) determining qualified task performers during an eRadiology process instance based on the role-to-task permission policy. In addition, the model should not incur any significant administrative overhead and should be self-administering to a great extent.

Table 1: Extract of authorization requirements for the healthcare process of Figure 1 (Task execution and application data access permissions).

1.	Physicians may issue radiological requests for their patients only. (Issue_Rad_Request)
1.1	Physicians may write radiological requests for their current patients.
1.2	Physicians may edit radiological requests for their current patients before sent.
1.3	Physicians may send radiological requests for their current patients.
1.4	Physicians may cancel radiological requests for their current patients after sent.
1.5	Physicians may read patient records of their patients only.
2.	Radiologists may issue radiological reports for patients on request by physicians. (Issue_Rad_Report)
2.1	Radiologists may read patient radiological requests issued by physicians
2.2	Radiologists may read patient records of patients they are requested to issue radiological reports for.
2.3	Radiologists may write patient radiological reports.
2.4	Radiologists may edit patient radiological reports before sent.
2.5	Radiologists may send patient radiological reports to the requesting physicians.
2.6	Radiologists may read past patient radiological reports prepared by them.
3.	Physicians may receive patient radiological reports issued by radiologists only if requested by them. (Receive_Rad_Report)
3.1	Physicians may read the radiological reports issued by radiologists on request by them.
3.2	Physicians may read patient records of their patients.

Given a cloud computing PHR architecture, where patient data are accessed via web services deployed through BPEL, these authorization requirements of the eRadiology process can be translated into authorization requirements with regard to web service invocations and associated task executions. These requirements include the following:

- **Restricted Web Service Invocation:** Web services for eRadiology and PHR access can only be invoked (executed) by a dynamically determined set of role holders subject to contextual constraints (e.g. user/patient proximity as well as location and time of attempted access).
- **Restricted Task Execution:** Given an authorization for invoking a web service, role holders can execute a dynamically determined set of web service tasks subject to contextual constraints (e.g. user/patient proximity as well as location and time of attempted access).

3 ACCESS CONTROL ARCHITECTURE

A major pain point in cloud computing is the lack of delegated authorization. While some cloud services provide for delegated strong authentication (e.g., Salesforce.com) that enables access control based on user identity, few, if any, provide delegated authorization to enable access control based on contextual information and user roles. This capability is turning out to be increasingly important as fine-grained entitlements for authorization management and control will be most essential. Hence, more granular authorization is needed. Authorization can be coarse-grained within an enterprise or even a private cloud, but in order to handle sensitive (such as medical) data and compliance requirements, public clouds will need granular authorization capabilities (such as role-based controls and IRM) that can be persistent throughout the cloud infrastructure and the data's lifecycle.

Figure 2 shows a high-level view of the security architecture implemented into NefeliRadiology. The access control mechanism uses collected contextual information to mediate between subjects (healthcare professionals) and objects (web services and associated tasks) to decide whether execution of an object by a given subject should be permitted or denied. The access control mechanism is certificate-

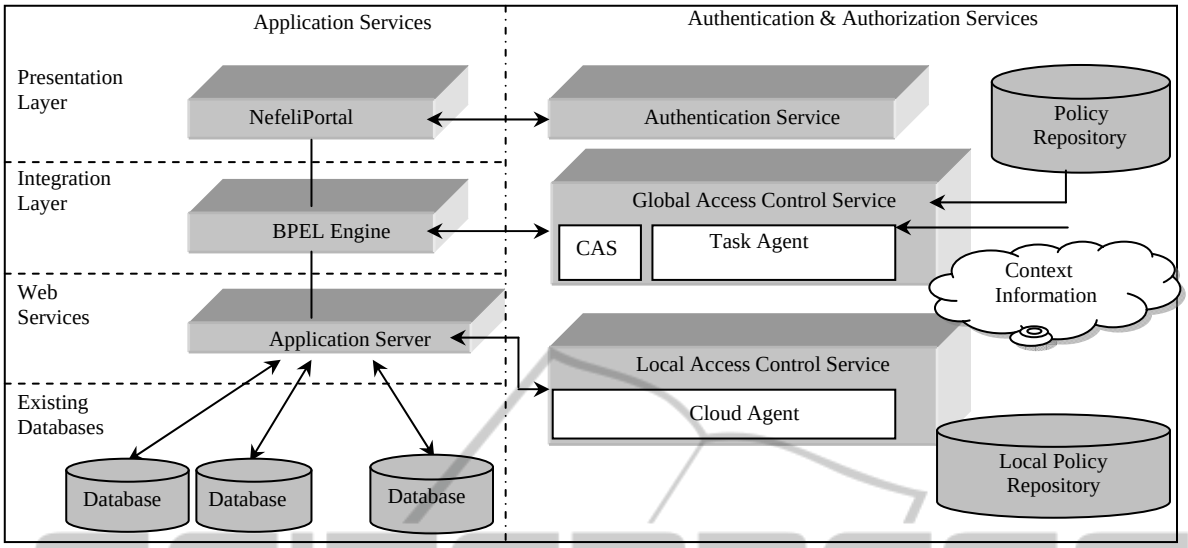

Figure 2: Security architecture in NefeliRadiology.

based as it relies on Community Authorization Service (CAS) certificates issued to healthcare professionals by a CAS server. These certificates specify user-to-role assignments in the form of security assertions, expressed in Security Assertion Markup Language (SAML) (Pearlman et. al., 2002). The role-to-permission (role-to-web service invocation and role-to-task execution) mapping is performed by means of access control policies expressed by using the RBAC profile of eXtensible Access Control Markup Language (XACML) (OASIS Standards, n.d).

For example, upon submitting a request for invoking a web service, the roles contained in the CAS certificate accompanying the request are extracted and their permissions regarding web service invocations are specified using a file where XACML policies have been stored. Then, during web service execution, a request for executing one of the associated tasks is issued which is accompanied by the same CAS certificate. The roles extracted from this certificate are used in order to specify the permissions regarding BPEL task executions using XACML policies which are stored at each client node (i.e. healthcare organization). Permissions on both web services and associated BPEL tasks are dynamically adapted by the constraints imposed by the current context.

In the NefeliRadiology prototype, the contextual information is determined by a pre-defined set of attributes related to the user (e.g. user certificate, user/patient relationship), to the environment (e.g. location and time of attempted access) and to the client or healthcare organization (e.g. local security policy). Contextual information is collected by a Context Manager which consists of two kinds of agents developed in JADE (Java Agent Development Framework, n.d.):

- **Cloud Agent:** Hosted on a cloud server and manages user permissions on web services.
- **Task Agent:** Hosted on a participating healthcare organization server and manages user permissions on BPEL tasks.

Each agent uses context collection services to monitor context and interacts with a state machine that maintains the permission subset of each role. The state machine consists of variables that encode state (permissions assigned to each role) and events that transform its state. Upon an attempted access (either to a web service or to an associated task), the relevant agent generates an event to trigger a transition of the state machine. Changes in user and environmental context are sensed by both agents, whereas changes in client context are sensed and dealt with by the cloud agent of each client node.

4 CONCLUSIONS

Development of cloud computing applications that provide readily access to healthcare information introduces security risks especially with regard to authorization and access control. One important healthcare delivery application is eRadiology which has been defined as the process of physicians (e.g. clinicians in hospital and ambulatory settings, general practitioners) directly entering radiological

requests using computer applications that provide decision support and can deliver the requests electronically in structured form to appropriate medical organizations (e.g. diagnostic centers, hospitals). Moreover, the radiological reports (incorporating image and text) are stored in a cloud infrastructure while granting relevant access rights to referring physicians. Hence, the term "eRadiology" has been used regardless of whether such radiological requests are subsequently printed and given to the patient, faxed to a medical center, or delivered through more structured electronic transfer. In this framework, the proposed security mechanism, embedded into an eRadiology cloud portal application, ensures authorized invocation of web services and execution of associated BPEL tasks subject to the constraints imposed by the execution context. One particular assumption of the proposed system specifically calls for the integration of eRadiology systems with PHRs and, possibly, other external systems since systems integration is a prerequisite for accurate safety alerts, patient monitoring and other recommended capabilities. The security framework proposed should aid eRadiology developers in comparing alternative systems and in prioritizing their development efforts. However, there is an obvious need for its real world validation before it is widely adopted. This requires setting up a cloud computing infrastructure for eHealth services, an endeavour that needs much more than proven technological feasibility.

REFERENCES

Andriole, K.P., Khorasani R., 2010. Cloud Computing: What Is It and Could it Be Useful?. *In Journal of American College of Radiology*, Vol.7, No. 4, pp. 252-254.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D.A., Rabkin, A., Stoica, I., Zaharia, M., 2009. Above the Clouds: A Berkely View of Cloud Computing. Technical Report No. UCB/EECS-2009-28, http://www.eecs. berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html.

Ash, J., Berg, M., Coiera, E., 2004. Some Unintended Consequences of Information Technology in Health Care: The Nature of Patient Care Information System Related Errors. *In Journal of the American Medical Informatics Association*,Vol. 11, No. 2, pp. 104-112.

Bell, D.S., Cretin, S., Marken, R.S., Landman, A.B., 2004. A Conceptual Framework for Evaluating Outpatient Electronic Prescribing Systems Based on Their Functional Capabilities. In *Journal of the American Medical Informatics Association*, Vol. 11, No. 1, pp. 60-70.

Benjamin, M., Aradia, Y., Shreibera, R., 2010. From shared data to sharing workflow: Merging PACS and teleradiology. In European Journal of Radiology, Vol. 73, pp. 3-9.

Bruening, P., Treacy, B, 2009. Cloud Computing: Privacy, Security Challenges. In The Bureau of National Affairs.

Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I., 2009. Cloud computing and emerging IT platforms:Vision, hype, and reality for delivering computing as the 5th utility. In *Future Generation Computer Systems*, Vol 25, pp. 599-616.

Cavoukian, A., 2008. Privacy in the clouds. In Identity in the Information Society, Vol. 1, No. 1, pp. 89-108.

Collin, S., Reeves, B.C., Hendy, J., Fulop, N., Hutchings, A., Priedane, E., 2008. Implementation of computerised physician order entry (CPOE) and picture archiving and communication systems (PACS) in the NHS: quantitative before and after study. In British Medical Journal, 337:a939.

Harvey, D., 2010. Record in the Clouds. In Radiology Today, Vol. 11, No. 2, p. 10.

IBM Cloud computing White paper, 2009. IBM Point of View: Security and Cloud Computing, ftp://public.dhe.ibm.com/common/ssi/sa/wh/n/tiw14045usen/TIW14045USEN_HR.pdf.

IBM Corporation, 2005. IBM Websphere Workflow – Getting Started with Buildtime V. 3.6.

Information Technology in Healthcare, 2004. Report to the Congress: New Approaches in Medicare, http://www.medpac.gov/publications/congressional_reports/June04_ch7.pdf.

Java Agent Development Framework, http://jade.tilab.com/.

Kaelber, D.C., Shah, S., Vincent, A., Pan, E., Hook, J.M., Johnston, D., Bates, D.W., Middleton, B., 2008. The Value of Personal Health Records, By the Center for Information Technology Leadership (CITL), http://www.citl.org/publications/_pdf/CITL_PHR_Report.pdf.

Metfessel, B.A., 2007. Financial and Clinical Features of Hospital Information Systems. In Healthcare Organizations, *Journal of Financial Management Strategies*, Vol. 2, No. 3.

Muttig I., Burton C., 2009. Cloud Security Technologies. In Information Security Technical Report, Vol. 14, pp. 1-6.

OASIS Standards, http://www.oasis-open.org/.

Pearson, S., 2009. Taking Account of Privacy when Designing Cloud Computing Services. Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, Vancouver, Canada.

Pearlman, L., Welch, V., Foster, I., Kesselman, C., Tuecke, S., 2002. A Community Authorization Service for Group Collaboration. Proceedings of the 3rd IEEE International Workshop on Policies for Distributed Systems and Networks, Monterey, USA.

Polymenopoulou, M., Malamateniou, F., Vassilacopoulos, G., 2005. Emergency Healthcare Process Automation

using Workflow Technology and Web Services. In International Journal of Medical Informatics, Vol. 28, No. 3, pp. 195-207.

Reid, W., 2010. Managing the Flow of Radiology. In Imaging Economics, May 2010.

Rosenthal, A., Mork, P. Li, M.H., Stanford, J., Koester, D., Reynolds, P., 2010. Cloud computing: A new business paradigm for biomedical information sharing. In Journal of Biomedical Informatics, Vol. 43, pp. 342-253.

Shimrat, O., 2009. Cloud Computing and Healthcare, San Diego Physician.org.

Steele, R., Lo, A., 2009. Future Personal Health Records as a Foundation for Computational Health, In Computational Science and Its Applications – ICCSA, Vol. 5593, pp. 719-733.

Telemedicine Information Exchange-TIE Europe., 2005. How e-radiology can help?, http://tie.telemed.org/europe/toolkits/kitdom.asp?load=toc&name=telerad.

Terry, M., 2008. Personal Health Records - Who are the key PHR providers and how are they handling laboratory results, Washington G2 Reports, http://www.g2reports.com/issues/advisory/advisory/mark_terry/345-1.html.

U.S. Department of Health and Human Services, Office of the Secretary, 2004. 45 CFR Part 162. Standard Unique Health Identifier for Health Care Providers. In Federal Register, Vol. 69, No. 15, pp. 3434–3469.

van der Burg, S., Dolstra, E., 2009, Software Development in a Dynamic Cloud: From Device to Service Orientation in a Hospital Environment. Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, Vancouver, Canada.