# Achieving Patient-Centered Fine-Grained Access Control in Hospital Information Systems
## *Using Business Process Management Systems*

Nahid AlThqafi, Hessah AlSalamah and Ahmad Daraiseh
*College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia*

Keywords: Access Control, Business Process Management (BPM), Electronic Medical Record (EMR), Hospital Information System (HIS), Patient-Centric Fine-Grained Access Control (PCFGAC).

Abstract: Access Control to patients' medical information in Hospital Information Systems (HIS) is a challenge in modern Patient-Centered (PC) healthcare. Fine–Grained Access Control (FGAC) in particular has been identified as one of the security requirements in these systems. In FGAC, only parts of medical information that are relevant and required by healthcare providers are accessed at the point of care. This cannot be achieved without a holistic view of a medical condition through a Patient-Centered Fine-Grained Access Control (PCFGAC), in which patient-centricity is considered. This research proposes using Business Process Management (BPM) to achieve PCFGAC in order to provide a real-time access control based on a "need-to-know" principle. Through a prototype that uses BPM, security requirements of PCFGAC were met. These include: authority control, informed decision support, fine-grained access control, and dynamic policies support. Thus, a contribution to the knowledge and practice has been introduced.

## 1 INTRODUCTION

Hospital Information System (HIS) is the key to improving healthcare quality (Wager et al., 2013, Hovenga and Grain, 2013, Bodhani, 2013). It provides healthcare specialists with instant access to real-time information about their patients. This information is found in Electronic Medical Records (EMRs), which include comprehensive information about medical services that were introduced to a patient.

EMRs are at the center of any healthcare service; its design and management have an enormous impact on the healthcare industry. Patients' EMRs reflect their mental illness, contagious diseases, sexual behavior, and other confidential information (Jingquan and Michael, 2010). Due to the confidentiality of EMRs' content, many privacy legislations and standard policies have been introduced in order to govern the use of medical information (Abbas and Khan, 2014), for example, in the USA there is the "Health Insurance Portability and Accountability Act" (HIPAA) and the "Health Information Technology for Economic and Clinical Health" (HITECH). Both HIPAA and HITECH introduce basic controls and safeguards to prevent medical information attacks. These controls addressed user and entity authentication, access control, audit control, transmission security, and non-repudiation. These controls are substantially needed to handle integrity, availability, and confidentiality issues of EMRs (Hui et al., 2014). Access controls, in particular, are the most important safeguard against unauthorized access since it defines the accessible information for each user (Gajanayake et al., 2012).

Controlling access rights to different portions of data is the key concept of Fine-Grained Access Control (FGAC). FGAC governs the access to data by each user of the system (Chatterjee et al., 2014, Harith and Gábor, 2009, Jinyuan and Yuguang, 2010, Liu et al., 2012, Yu et al., 2010, Rizvi et al., 2004) based on the "need-to-know" principle. The lack of FGAC is an open problem in HISs. Despite the large amount of research dedicated for modeling the requirements of EMR access control mechanisms, there are limited results that focus on the development of an implementation scheme to enforce access control in HIS (Chen et al., 2010). This is because the healthcare access control systems are naturally fine-grained and dynamic (Chen et al., 2010). Thus, there is a real need to enforce access control beyond the



AlThqafi, N., AlSalamah, H. and Daraiseh, A.
Achieving Patient-Centered Fine-Grained Access Control in Hospital Information Systems - Using Business Process Management Systems.
DOI: 10.5220/0005630200390048
In *Proceedings of the 9th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2016) - Volume 5: HEALTHINF*, pages 39-48
ISBN: 978-989-758-170-0

functional-level to consider the content of the accessed data.

Our perspective for Patient- Centered (PC) healthcare is: "A collaborative effort… where patients and the health care professionals collaborate as a team, share knowledge and work toward the common goals of optimum healing and recovery" (Alsalamah et al., 2013). We believe that considering the treatment flow and its different stages in addition to the patient's condition will improve both the healthcare provision (AlSalamah et al., 2012) and the protection of the patient's privacy. Doing so will provide ongoing monitoring and auditing through each step of the treatment process as it is executed. This enables Patient-Centered Fine-Grained Access Control (PCFGAC) that respects both dynamic and real-time requirements of HIS.

Moving HISs from the functional model into the process-oriented model makes them more flexible and adaptive to changes in real-time manner. This emphasizes the value that process-oriented models, such as Business Process Management (BPM), can add to such systems. This is because using BPM enables the management of each step of the process by controlling its input, output, performer and rules according to the condition of each individual case.
The adaption is required to provide an appropriate PCFGAC that respects the dynamic nature of EMR security requirements for each patient. In addition, BPM can deal with the information repositories (such as HIS databases) not only for storing and retrieving information, but also for supporting different views according to the treatment required for each individual (Brucker and Hang, 2013); (Reddy and Dourish, 2002).

This research aims to create an integrated framework for modeling, analyzing and enforcing security and privacy requirements. It uses BPM as an Active Enforcement (AE) (Agrawal et al., 2007) which will be implemented as an independent middleware solution (see figure 1), that allows the data-owners to protect their data from disclosure by enforcing new policies in real-time.

These real-time policies build up as the patient passes through the treatment stages in order to adapt to emerging privacy and security needs according to each patient's medical condition.
The policies take place between user interface and HIS's databases (as shown in figure 1) to ensure that any access to patient information happens according to the information-owner's preferences, and applicable access control rules.

AE will help in managing access to data in a secure manner to protect its privacy. BPM also manages access at the cell level in the database, rather than just at the row or the column level, which facilitates the provision of PCFGAC.

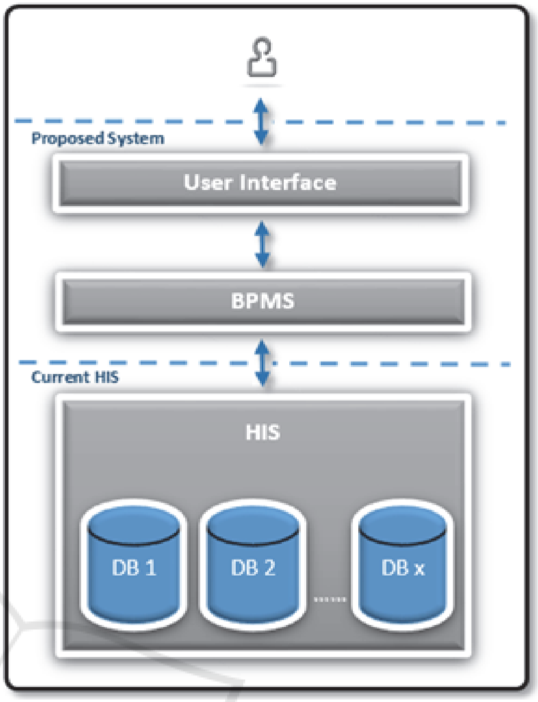



Figure 1: Proposed System Architecture.

So, utilizing BPM as an AE will provide the following key strengths:

- A methodology capable of handling both system policies and user's preferences (healthcare provider or patient). These preferences are taken according to the specific needs for each patient separately.
- It will enforce system's policies and user's preferences through BPM's user interfaces based on the context of the treatment.
- PCFGAC will be provided; by taking each case condition into account in the enforcement of FGAC.

The following section in this paper will present the gap in the literature presenting previous studies that address FGAC and uses of BPM. This will be followed by the methodology used to conduct this research. In the fourth section, the development of proposed prototype will be introduced, and the results will be discussed in section five. Finally, section six discusses future work and concludes the research.

## 2 RELATED WORK

Patients require proper use of their health information which cannot be achieved without implementing FGAC (Jinyuan and Yuguang, 2010). Generally, parts of the patient's medical record are more sensitive than others. While most access control mechanisms look at privacy control of a record in terms of a block of fields, patients may wish to keep some fields more private than others in their medical record(Samuel and Zaiane, 2012). Thus, achieving FGAC was addressed in many studies. Most of the studies in the literature achieve FGAC through Role-Based Access Control (RBAC) with some enhancements (Amato et al., 2013, Chen-Guang et al., 2011, Steele and Kyongho, 2010). Steele and Kyongho (Steele and Kyongho, 2010) enhanced the traditional RBAC by identifying the sensitivity levels that had been specified for each portion of the accessed data. On the other hand Amato et al. (Amato et al., 2013) coupled the traditional RBAC mechanism with access control restrictions that are defined as IF-then rules. Other researches enforce FGAC on the database level instead of application level, which provide access control on the row or even cell level (Harith and Gábor, 2009). Chatterjee et al. (Chatterjee et al., 2014) achieved FGAC by defining users' privileges based on logic expressions for each object's attribute. Hui et al., (2014) introduced attribute access control by using attribute-encryption in addition to privilege separations mechanisms. These studies did not consider the dynamic nature of accessed data at execution time. Thus, these solutions provide a rigid system that deal with all cases at active time in the same way. They highly depend on fixed access rules constructed at design time. A flexible access control that meets each need of each individual is required in the healthcare domain.

Improving the access control's flexibility in HISs had been addressed by many researchers. Chen-Guang et al., (2011) enhanced RBAC by dividing the inner structure of the user and by using the token concept to provide an access control that meets the dynamic access control demands. Hu (Hu and Weaver, 2004) implemented dynamic and context-aware access control in distributed healthcare applications by applying the concept of "least privilege" to ensure that any user is unable to access more authorized rights than what he/she needs for executing the requested service. They developed two algorithms that can be dynamically invoked at runtime to evaluate the context by using six parameters (time, location, IP address, user ID, object type, and object ID). Leyla and McCall (Leyla and MacCaull, 2012) enhanced a Personal Access Control (PAC) model, which allows patients to control the access rights to their health records. They used a workflow mechanism to build a prototypical framework that captures patient permissions and enforces PAC policies. Three aspects have been addressed in their proposal: incorporation of a patient permission with access control mechanism, "need-to-know" principle, and delegations. Russello et al. (2008) also introduced a workflow based access control framework to produce a flexible access control mechanism in e-health applications to adapt access rights of the actual task. Their framework integrated authorization model (policy language) with a workflow management system (WFMS) to provide fine-grained control. In our proposal, we suggest the use of a Business Process Management System (BPMS) instead as it can deal with loosely structured processes in a dynamic environment such as healthcare (Van Der Aalst et al., 2003).

BPMS enables flexibility to build dynamic access controls since it manages and controls each case separately. Some research focused on the feasibility of BPMS to handle security issues. Long et al., (1999) addressed the dynamic access control requirements by considering the workflow system that enables the development of high-level policies executed through system workflow. Liu et al., (2012) considered the access context differently to reach a mechanism that achieved context-aware FGAC. Levina et al., (2010), exploited BPM as a tool to help an information system's analysts identify the potential business rules. Ayoub et al., (2012) proposed semantic means to model access control explicitly in business process models. Brucker and Hang (Brucker and Hang, 2013) proposed a business process-driven system that created an integrated framework for modeling, analyzing and enforcing security, privacy and trust requirements. The workflow technology benefits will be achieved since "BPM is a subset of Workflow with more control over processes, integration and optimization" (Al-Salamah, 2011).

Although addressing security requirement using BPMS has been presented in the literature, it is still an open research area in the healthcare sector in particular. However, the use of BPM has been investigated in the healthcare domain for other usages. Matic and Andrej (Matic and Andrej, 2010) discussed the increasing adoption of BPM in the healthcare domain and its challenges. They found that the healthcare process is similar to the manufacturing process, which encouraged the adoption of BPM. Nevertheless, they concluded that there is a clear increase in the use of BPM in the healthcare domain, especially for disease control and clinical pathways processes. However, BPM adoption in the healthcare domain is slower than other domains because of its complexity and parallel and high variation in healthcare processes. Based on the thorough study of the literature, we believe that utilizing BPM to achieve PCFGAC in HISs is still in its infancy. BPMS can enforce access control at runtime, which adopts the dynamic requirements of each patient according to his/her specific condition. Thus, BPMS facilitates monitoring and controlling each stage of the treatment process during implementation. This helps meet the privacy requirements through controlling access rights of each step based on the “need- to-know” principle. That provides the needed PCFGAC in HIS.

# 3 METHODOLOGY

Design Science Research Methodology (DSRM) has been followed to provide incorporate principles, practices, and procedures required to carry out this research. It also obtains a nominal process model and a mental model for presenting and evaluating the research. The DS process followed involved “six steps: problem identification and motivation, definition of the objectives for a solution, design and development, demonstration, evaluation, and communication” (Peffers et al., 2007).

After identifying the problem and motivation, defining the objective and suggesting the solution in the previous sections, the following sections will cover the proceeding DS stages.

# 4 DESIGN & DEVELOPMENT

A proof-of-concept prototype was implemented to show how different access controls could be enforced by BPMS based on the medical condition. The heart failure treatment pathway was mapped as an exemplar with different possibilities of HIV test results, representing patients with comorbidity. The developed prototype was then evaluated, and results were communicated.

Bizagi BPM (Bizagi, 2014) was used to build the prototype. It required Microsoft SQL server to create an internal database and Internet Information Service (IIS Express) to provide a work portal used for both users' interfaces interactions and administrator’s maintenance. Both the Heart failure treatment process and HIV test process were designed, modeled and automated on Bizagi BPM. The prototype provided a framework to manage patients' medical information in a way that protects their privacy while ensuring its availability to support informed decisions by health providers involved along the treatment journey. Each treatment stage on the processes was controlled by limiting its access to the involved user who retrieves only the relevant information to act according to his assigned role in the treatment process (“need to know” principle).

Different cases were handled differently, representing unique medical conditions. This was achieved in the process through numbers of business rules that had been defined showing how the system adapts to the needs of each condition.

## 4.1 Heart Failure Treatment Process

The heart failure treatment process modeled is based on the treatment guidelines published by the UK, Map of Medicine health-guides (MoM) (Map of medicine, 2014).

These guidelines represent best practices and are used as an up-to-date, quality standard and related information that could be used as a recommendation on any health matter. The prototype model includes all activities that heart failure patients may pass through during their visit to a hospital as a walk-in or an outpatient. The model considered a hospital that is large enough to hold Laboratory, Radiology, and Pharmacy departments. Activities are shown in Figure 2.

The process has two start points: either by the receptionist as a default or by a cardiologist after consultations. The receptionist retrieves all booked appointments for the heart failure patients on a specific date.

Then he/she submits the arrived patient to the examination room where a nurse examines the patient and inserts the examination data into the system. Then, the patient’s case is submitted to the cardiologist who can view a comprehensive medical record about the patient (examination data, tests, visits, medications), in addition to his/her demographic data. Following this, according to the patient’s history and his/her symptoms, the cardiologist decides whether a BNP test is required or not; also, he may request an Echocardiogram.

Four cases are taken into account as shown in Figure 3.

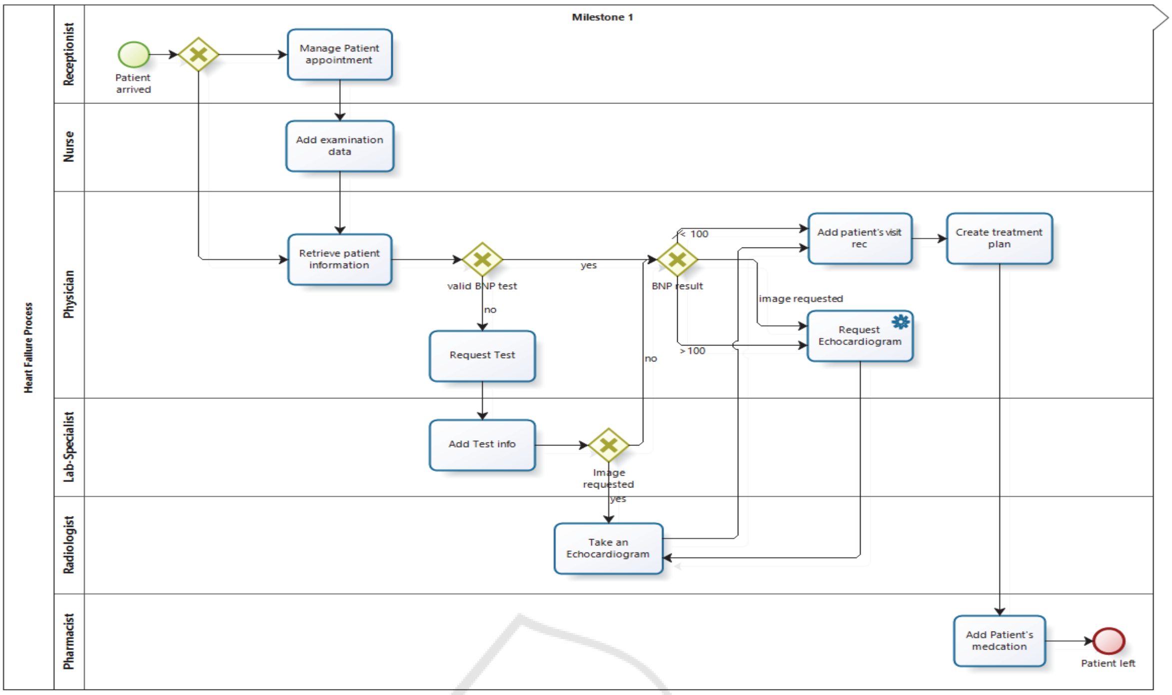



Figure 2: Heart Failure Pathway Process Executional Model.

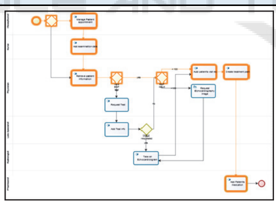
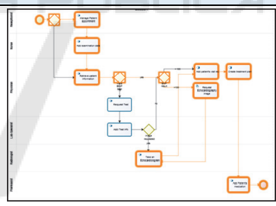
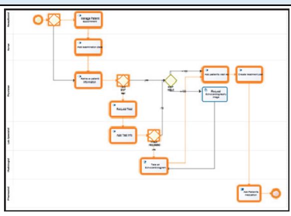
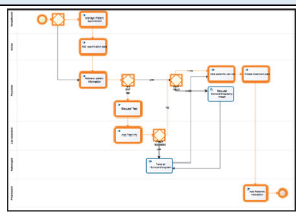
| No heart failure suspected, or Valid BNP Test is included within patient medical history | |
|---|---|
| **Case 1**: Patient's records show there is a valid BNP-test, and an Echocardiogram is available (no need to re-take the test). Also, the result of the valid BNP-test that exists **< 100** or no heart failure is diagnosed. | **Case 2**: Patient's record shows that a valid BNP-test is available, but its result is greater or equal to **>= 100**. In this case, an Echocardiogram is required. |
|  |  |
| **Heart failure is suspected; BNP test is needed, and no valid one exists** | |
| **Case 3**: Patient's records show BNP or Echocardiogram are not valid or available. In this case, both are requested from a cardiologist. Or only a BNP and its result is > 100, and an echocardiogram will be requested. | **Case 4**: Only BNP is needed and its result <100 |
|  |  |

Figure 3: Paths of HF's cases.

### 4.2 HIV Test Process

HIV test process represents the pathway activities as suggested by Map of Medicine (MoM) (Map of medicine, 2014).

Three parties are involved in this process: the lab specialist who performs the test and insert its result, the HIV clinic assessor who assesses the patient's condition and provides therapy, and the Psychologist who monitors and supports the psychological aspects for the HIV patients. HIV test process activates are shown in Figure 4.

HIV test process starts when the Lab specialist receives an HIV test request, performs the test and inserts its result into the system.

Two cases are taken into account in this process: in cases where there is a positive HIV-test result, the case will be transferred to the HIV clinical assessor where more tests and psychological referral are required. The psychologist's role is to support the patients psychologically to improve their quality of life. Based on the output of performed tests and psychologist assessment, the HIV clinic will start the suitable Highly Active Antiretroviral Therapy (HAART).

However, in cases where the result is negative, the system will terminate the process. Figure 5 shows different paths for the HIV test pathway.

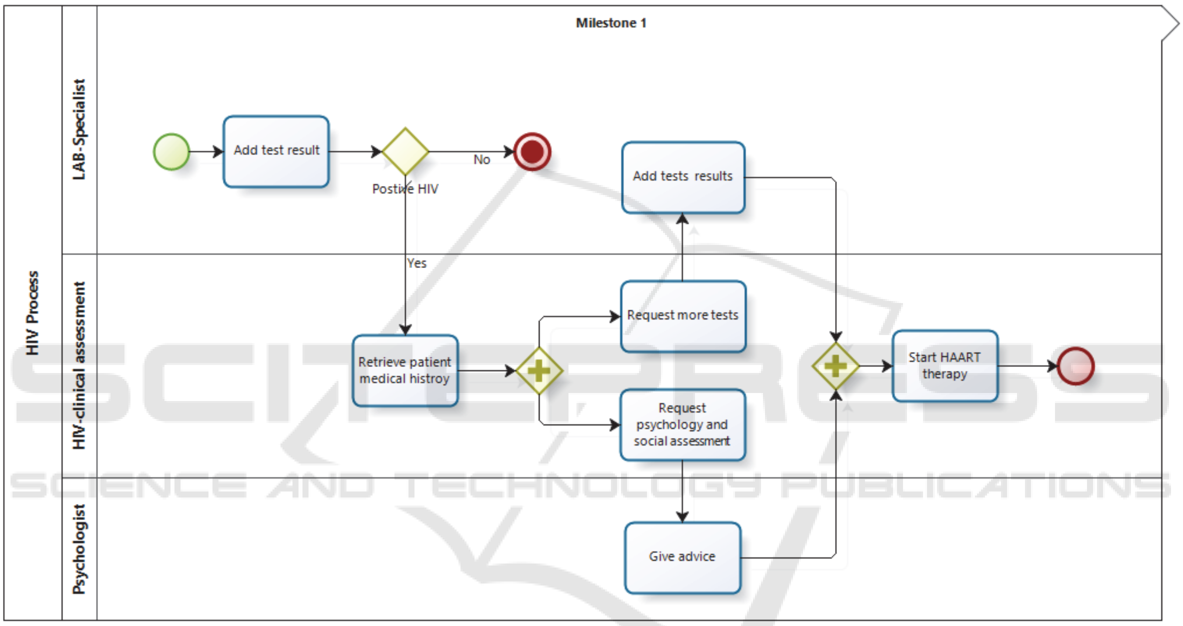





Figure 4: HIV-test Pathway Process Executional Model.

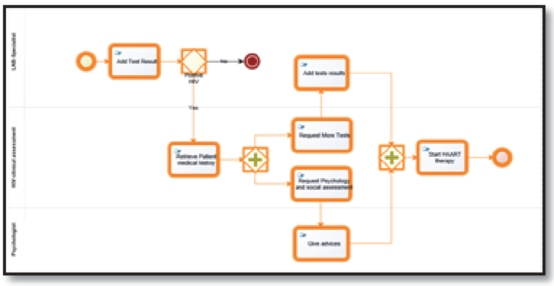
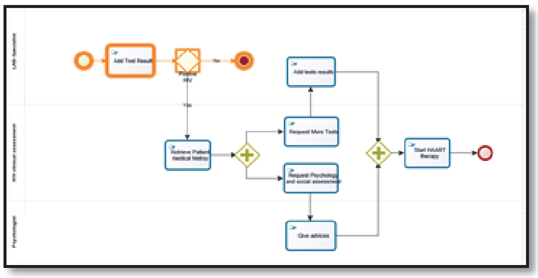
| HIV-test is requested | |
|---|---|
| **Case 1:** Positive-HIV Patient. | **Case 2:** Negative-HIV Patient |
|  |  |

Figure 5: Paths of HIV-test cases.

## 4.3 The Effect of HIV-test Process on Heart Failure Treatment Process

When patients are suffering from multiple diseases (with comorbidity), the system adapts to the needs considering all relevant issues.

In the model, when a patient goes through both Heart Failure and HIV processes at the same time, the information appearance in the Heart Failure process will be affected by the result of the HIV-Test process.

All of the patient's personal information will be hidden in the user's interfaces when a positive-HIV result is found. Figures 6 and 7 show the different views that the cardiologist and lab-specialist can obtain when a BNP-test is needed for a Heart Failure patient. Figure 7 shows the medical record has been anonymized and the relevant warning message has been displayed.


Figure 6: Cardiologist/Lab-specialist view for Negative-HIV patient.

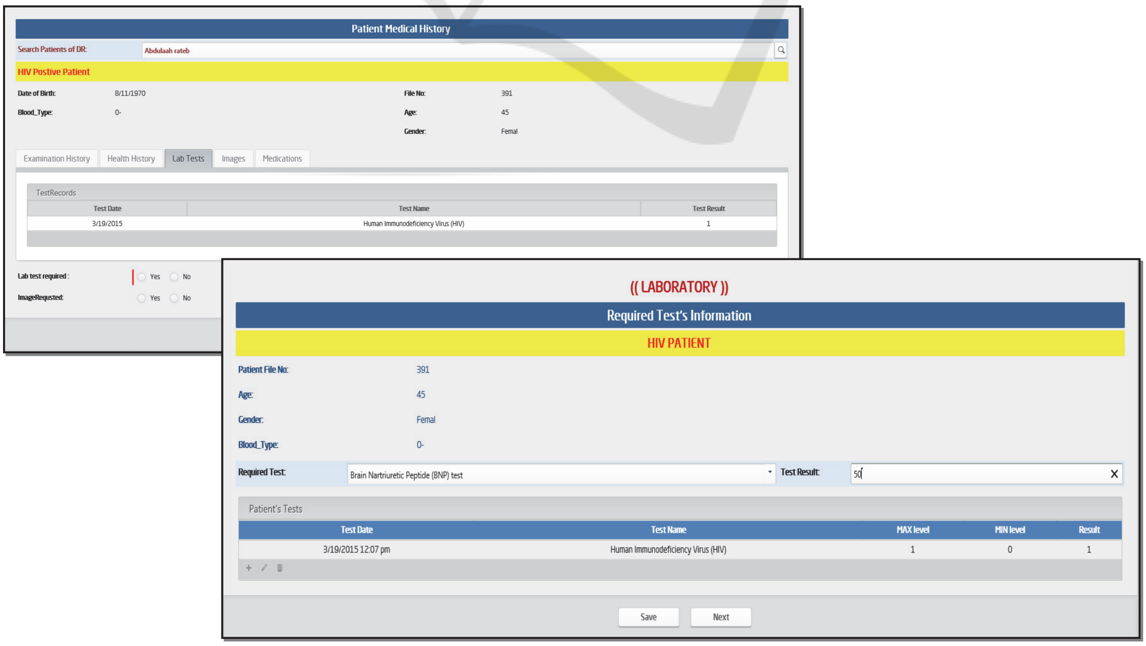



Figure 7: Cardiologist/Lab-specialist view for Postive-HIV patient.

# 5 RESULTS AND DISCUSSION

The prototype showed that, the provision of PCFGAC in HISs can be achieved using BPMS. PCFGAC was achieved through the facilitated features of BPMS, and these include:

## 5.1 Authority Control

Authority control facilitates through:

### 5.1.1 Role-based Access Control

Unauthorized access prevention is achieved by using a classification scheme for both users and patients' information. Users are classified into eight domains/roles: Receptionist, Nurse, Doctor, Lab specialist, Radiologist, Psychologist, HIV assessor and Pharmacist. The permission granted to each user is limited to his role to view, add or delete the related information that is needed to perform their role in the treatment process.

Data Structure is built based on the data's nature. It was divided into eight main tables: Demographic Data, Appointments, Examination Data, Patient's Tests, Patient's Images, Patient's Medications, Psychological date and Patient History (visits details). The model maps each of its users to the related table(s) that are necessary as a resource(s) to perform his/her role in the treatment process. Moreover, users with the same role have different views according to the sensitivity of the process itself (for example, HIV test process) or the contained information (for example, patient with positive HIV).

Furthermore, accessing patient records is limited only by an engaged cardiologist, which means other cardiologists with the same role cannot view the medical record.

### 5.1.2 One-time Access Control

Access is granted at execution time. Authorization is permitted at the level of an exact action, and only to the active task when a task representing a treatment stage is reached. When a task is active, authorization is allowed to the relevant user and only for a specified duration. When the treatment stage is accomplished, following this temporary period, the task in the user inbox disappears.

## 5.2 Informed Decisions Support

Using BPMS supports the informed decisions that should be taken by healthcare providers through providing them with the following:

### 5.2.1 Real-time Information

The health information model supports health providers to make informed decisions by providing up-to-date real-time information. This is as information is fetched from the original resources at the treatment stage. E.g. a lab test result, when needed, is accessed from the laboratory database without waiting for these reports to be sent to physicians.

### 5.2.2 Historical Information

Retrieving the medical history of a patient helps make an informed decision based on a holistic view of the condition. An example of a straightforward benefit would be avoiding potential drug interactions or contraindications. Other benefits include all complications associated with comorbidity and demographic details which make each patient's condition unique.

### 5.2.3 Relevant Information

A filter process is applied according to the guidelines to ensure that relevant real-time and historical information that supports the treatment stage is represented.

## 5.3 Fine-Grained Access Control

Access rules in the model shaped Fine-Grained access control by deciding who can access which data and when. This done for each step of the processed case individually.

### 5.3.1 Patient-specific Access Control

Different paths are available in the model; each path directs the case to the different user according to its condition. Different views according to the accessed data are also considered during user's interfaces' design.

### 5.3.2 BPMS Features

BPMS tool provides a wide range of features: the information visibility, filters, mandatory and editable. These add-on features help control the views and accesses of the data fields in the user interface based on the defined business rules.

### 5.3.3 Dynamic Security Policies Support

The context of each case leads to different access decisions according to the access rules that respect both case condition and accessed data. For example, an Echocardiogram request is based on three factors: the value of BNP test's result, unavailability of a valid Echocardiogram in the patient's images history, and the cardiologist request to perform that test.

Moreover, BPMS provides a monitoring feature in which users can track the process progression at any stage. Furthermore, they may determine the bottlenecks that may hinder or affect a successful execution of the process, which can be used to improve the whole process.

To sum up, BPMS grants that only the correct user accesses the required information to make the correct task/decision at the right time in a case-specific matter.

# 6 FUTURE WORK & CONCLUSION

The aim behind this study was to satisfy security requirements in the healthcare domain. The focus was on the PCFGAC and the advantages that could be achieved using BPMS. The work here could be extended to include an information privacy classification scheme and information security awareness support.

Inclusion of technology to enhance the outcome could also be studied through a thorough study of the benefits that could be achieved if we had the PCFGAC model on the cloud. Other benefits that do not directly feed the security needs could also extend this work. This includes the independency of the AE layer and the possibility to maintain and evolve the model as the treatment guidelines or delivery are updated.

In conclusion, PCFGAC model is a prototype that proves that BPMS can represent a treatment pathway with an acceptable degree of efficiency and effectiveness. FGAC was achieved through the classification of users' and patient information in the model. Also, PC requirements were met by using the features that BPMS facilitated. These include: authority control, informed decision support, fine-grained access control, and dynamic security policies support. Thus, a contribution to the knowledge and practice has been introduced.

# REFERENCES


Abbas, A. & Khan, S. U. 2014. A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds. *Biomedical and Health Informatics, IEEE Journal of,* 18**,** 1431-1441.

Agrawal, R., Grandison, T., Johnson, C. & Kiernan, J. 2007. Enabling the 21st century health care information technology revolution. *Communications of the ACM,* 50**,** 34-42.

Al-Salamah, H. 2011. Velindre Hospital Integrated Care Pathway Gold Award: Medical and Healthcare Nominated by Cardiff School of Computer Science and Informatics, Cardiff University, UK. *In:* Swenson, K. D., Palmer, N. & Silver, B. (eds.) *Taming the Unpredictable: Real World Adaptive Case Management: Case Studies and Practical Guidance.* Future Strategies Inc.

Alsalamah, H., Gray, A. & Morrey, D. 2012. Mapping the integrated care pathway into bpm for health case management. *S-BPM ONE-Education and Industrial Developments.* Springer.

Alsalamah, S., Gray, W. A., Hilton, J. & Alsalamah, H. Information security requirements in patient-centred healthcare support systems. MedInfo, 2013. 812-816.

Amato, F., Mazzocca, N., DE Pietro, G. & Esposito, M. A System for Semantic-Based Access Control. P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2013 Eighth International Conference on, 28-30 Oct. 2013 2013. 442-446.

Ayoub, M. F., Hassan, R. & Elmongui, H. G. ESAC-BPM: Early Security Access Control in Business Process Management. ICSEA 2012, The Seventh International Conference on Software Engineering Advances, 2012. 650-655.

Bizagi, 2014 [Online]. Available: http://www.bizagi.com.

Bodhani, A. 2013.Warding off fraud. *Engineering &Technology,* 8**,** 36-39.

Brucker, A. D. & Hang, I. Secure and compliant implementation of business process-driven systems. Business Process Management Workshops, 2013. Springer, 662-674.

Chatterjee, S., Gupta, A. K., Mahor, V. K. & Sarmah, T. An efficient fine grained access control scheme based on attributes for enterprise class applications. Signal Propagation and Computer Technology (ICSPCT), 2014 International Conference on, 12-13 July 2014 2014. 273-278.

Chen-Guang, H., Cun-Zhang, C. & Shu-DI, B. An Enhanced Role-Based Access Control Mechanism for Hospital Information Systems. Computational Intelligence and Security (CIS), 2011 Seventh International Conference on, 3-4 Dec. 2011 2011. 1001-1005.

Chen, K., Chang, Y.-C. & Wang, D.-W. 2010. Aspect-oriented design and implementation of adaptable access control for Electronic Medical Records. *International journal of medical informatics,* 79**,** 181-203.

Gajanayake, R., Iannella, R. & Sahama, T. R. Privacy oriented access control for electronic health records. Data Usage Management on the Web Workshop at the Worldwide Web Conference, 2012. ACM.

Harith, I. & Gábor, H. 2009. Fine-Grained Data security in Virtual Organizations. *Database Technologies: Concepts, Methodologies, Tools, and Applications.* Hershey, PA, USA: IGI Global.

Hovenga, E. J. S. & GRAIN, H. 2013. Health information systems. *Studies In Health Technology And Informatics,* 193**,** 120-140.

Hu, J. & Weaver, A. C. Dynamic, context-aware access control for distributed healthcare applications. Workshop on Privacy, Security, and Trust, 2004.

Hui, Z., Rong, H., Ximeng, L. & Hui, L. Spemr: A new secure personal electronic medical record scheme with privilege separation. Communications Workshops (ICC), 2014 IEEE International Conference on, 10-14 June 2014 2014. 700-705.

Jingquan, L. & Michael, J. S. 2010. Electronic Medical Records, HIPAA, and Patient Privacy. *Health Information Systems: Concepts, Methodologies, Tools, and Applications.* Hershey, PA, USA: IGI Global.

Jinyuan, S. & Yuguang, F. 2010. Cross-Domain Data Sharing in Distributed Electronic Health Record Systems. *Parallel and Distributed Systems, IEEE Transactions on,* 21**,** 754-764.

Levina, O., Holschke, O. & Rake-Revelant, J. Extracting business logic from business process models. Information Management and Engineering (ICIME), 2010 The 2nd IEEE International Conference on, 16-18 April 2010 2010. 289-293.

Leyla, N. & Maccaull, W. 2012. A Personalized Access Control Framework for Workflow-Based Health Care Information. Berlin, Heidelberg: Springer Berlin Heidelberg.

Liu, H.-Y., Deng, M.-L. & Yang, W.-D. A Context-Aware Fine-Grained Access Control Model. Computer Science & Service System (CSSS), 2012 International Conference on, 11-13 Aug. 2012 2012. 1099-1102.

Long, D. L., Baker, J. & Fung, F. A prototype secure workflow server. Computer Security Applications Conference, 1999. (ACSAC '99) Proceedings. 15th Annual, 1999 1999. 129-133.

Map of medicine (MOM), 2014 [Online]. Available: http://healthguides.mapofmedicine.com/choices/map/index.html.

Matic, M. & Andrej, B. 2010. Electronic Environments for Integrated Care Management Case of Depression Treatment. *Ubiquitous Health and Medical Informatics: The Ubiquity 2.0 Trend and Beyond.* Hershey, PA, USA: IGI Global.

Peffers, K., Tuunanen, T., Rothenberger, M. A. & Chatterjee, S. 2007. A design science research methodology for information systems research. *Journal of management information systems,* 24**,** 45-77.

Reddy, M. & Dourish, P. A finger on the pulse: temporal rhythms and information seeking in medical work. Proceedings of the 2002 ACM conference on Computer supported cooperative work, 2002. ACM, 344-353.

Rizvi, S., Mendelzon, A., Sudarshan, S. & ROY, P. Extending query rewriting techniques for fine-grained access control. Proceedings of the 2004 ACM SIGMOD international conference on Management of data, 2004. ACM, 551-562.

Russello, G., Dong, C. & Dulay, N. A workflow-based access control framework for e-health applications. Advanced Information Networking and Applications-Workshops, 2008. AINAW 2008. 22nd International Conference on, 2008. IEEE, 111-120.

Samuel, H. W. & Zaiane, O. R. PSST… privacy, safety, security, and trust in health information websites. Biomedical and Health Informatics (BHI), 2012 IEEE-EMBS International Conference on, 5-7 Jan. 2012 2012. 584-587.

Steele, R. & Kyongho, M. HealthPass: Fine-Grained Access Control to Portable Personal Health Records. Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on, 20-23 April 2010 2010. 1012-1019.

Van der Aalst, W. M., Ter Hofstede, A. H. & Weske, M. 2003. Business process management: A survey. *Business process management.* Springer.

Wager, K. A., Lee, F. W. & Glaser, J. P. 2013. *Health Care Information Systems: A Practical Approach for Health Care Management*, Jossey-Bass.

Yu, S., Wang, C., Ren, K. & Lou, W. Achieving secure, scalable, and fine-grained data access control in cloud computing. INFOCOM, 2010 Proceedings IEEE, 2010. Ieee, 1-9.