Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 196 (2022) 509–516

Procedia
Computer Science

www.elsevier.com/locate/procedia

CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies 2021

Integrated privacy decision in BPMN clinical care pathways models using DMN

Intidhar ESSEFI*[a], Hanene BOUSSI RAHMOUNI[b], Mohamed Fethi LADEB[c]

[a]Higher Institute of Medical Technologies of Tunis (ISTMT) Tunis El Manar University, Tunisia
[b]University of the West of England, the Computer Science Research CenterBristol, UK
[c]Radiology Department, Kassab Orthopedics Institute, Manouba, Tunisia

Abstract

Personal data is highly affected by the witnessed digital transformation of healthcare processes. This process relies deeply on the connectivity and decentralization of healthcare systems and data repositories. In this context, value creation and quality enhancement are obviously leveraged, however both health providers and individuals could be exposed to many risks ranging from privacy violations to medical identity theft and personal harm. Hence, it is essential that healthcare stakeholders ensure privacy protection and systemic compliance to personal data regulations such as HIPPA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation). Taking clinical processes as a starting point is very important to highlight the personal data in use and to assess whether such usage is justifiable and subsequently allow privacy management decisions to be made. In this paper we combine BPMN (Business Process Model and Notation) and DMN (Decision Model and Notation) to model clinical care pathways as standard business processing constituting the hospital information system. Business process modelling presents a useful mean to model clinical care pathways. It allows a complete discovery of data processing scenarios. DMN (Decision Model and Notation) is implemented in BPMN models to present the rules that lead to a decision in easy-to-read tables which are executed directly by a decision engine. In addition, the integration of verifiable security labels of the manipulated data, we make sure compliance to legislation is ensured at the level of decision rules for each decision table of the DMN.

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
E-mail address: essefi.intidhar@gmail.com

10.1016/j.procs.2021.12.043

Keywords: BPMN, care pathways, Digital transformation, DMN, GDPR, HIPAA, protection methods, security labels, sensitive data.

1. Introduction

The witnessed digital transformation of hospitals and healthcare entities as well as their business processes have noticeably improved the healthcare quality. The first concern of governments after the digitalization revolution in the medical field is to preserve the patient's privacy and integrity. As the electronical exchange of data increases the threatening risk of illegal disclosure and misuse of the patient's information, protection personal data has become a central axe of the hospital information systems' security layer. In this context, data security and trust are serious challenges every healthcare entity is aiming to achieve. Achieving complete integration of hospital information systems in all medical practices and fields exposes the used personal data through the rolling care pathway processes to seriously increasing security threats and illegal disclosure. Hence, exchanging data in a secure and trusted way is crucial. Therefore, healthcare organization are witnessing a continuous medical practices transformation to be compliant with data protection laws and regulations such as HIPAA Privacy Rule [1] and GDPR It is also required that these organization maintain compliance once it is obtained since policies are increasingly dynamic.

Modelling care pathways processes using business processes models allows a transparent presentation of tasks and process participants. As BPMN offers a legible and reliable presentation of models, it's the most used standard for modelling detailed care pathways processes as needed. The main convenient of the BPMN standards is the lack of tools for presenting requirements and decisions on protecting sensitive data elements according to specified classification or characteristic. This explains the need for a decision-making language as the DMN alongside the BPMN standard. It is worth noting that DMN is used for precise specifications of business rules and decisions [3, 4].

Decision modelling is carried out in order to understand and define the decisions used in the organizations' business processes. The DMN use could be discerned in three main contexts: (1) for modelling human decision-making, (2) for modelling the requirements for its automation and (3) for implementing the automated decision-making. By defining specific tasks and activities within which the decision-making takes place, BPMN models could describe the coordination of decision-making within processes while the decision representation features are used to define the logic for making individual decisions [5]. In this work, we are proposing a data management approach based on policies compliance in order to make decision about sensitive data protection rules. This is based on BPMN models combined with DMN tables. We annotate data with carefully designed security and privacy tags to be able to implement decisions and govern data sharing throughout the processes.

Our contributions in this paper include:

- Model a BPMN model characterizing care pathways-related data for decision making about the medical data protection.
- Derive DMN decision models from the processes' incoming data for protecting medical data in compliance with the HIPAA Privacy Rule.
- An adapted protection model for care pathways following recommended legal framework for protecting personal data.
- An implementation of a medical data protection approach while developing the privacy by design concept for a future Hospital Information System development.

The remainder of this paper will be organized as follows. Section one presents the background and the related work. In section two, we present the HIPAA requirements for protecting personal data. In section three, we describe the material and methods part. As for section four, we present the use case in which we present the sensitive medical data protection in the imaging using BPMN combined with DMN decision modelling Then, we deal with results and discussion in section five. And finally, we sum up with the conclusion and the future work.

2. Background and related work

Medical care pathways are non-deterministic processes. They combine various factors, tasks, participants and uses. With the increasing need of improving the quality and the productivity of healthcare services, care organizations are in great need of formalization and standardization of their care pathways business processes. The implementation of

Hospital Information Systems (HIS) allowed a broader application of automating care pathways and higher productivity of healthcare operations [6-8]. This increases the risk of illegal disclosure and use of the processed data. Therefore, (1) protecting sensitive data has become a challenging issue the care provider organization and (2) its crucial to be compliant to the protecting requirements of policies and legislation as HIPAA and GDPR.

BPMN is a standardized notation for modelling business processes for clinical care pathways and for their automation throughout HIS' implementation and integration in medical data management. This standard was made to model deterministic and highly standardized processes as those of the medical field [9]. Despite its wide use, modelling business processes lacks the detailed presentation of the security and decision levels which are highly recommended in care pathways specially while disclosing the identifiable individual data. As for the DMN, it is a standard which is established by the OMG (Object Management Group) through other standards like BPMN and UML (Unified Modeling Language). Using an easy-to-read table, rules leading to a decision could be easily modelled. As well as decision making could be depicted in diagrams. The DMN allows a simplified presentation dedicate to model the decision logic and their requirements to complement business process [5, 10, 11].

BPMN and DMN are linked which makes it possible to separate business processes and decision-making and model them in specific diagrams with their specific language. Another objective is to ensure that the business rule models are interoperable and can be represented in XML and thus be able to be interpreted by different software tools. The BPMN combination with DMN models allows to naturally model decision logic separately from process logic which facilitates concerns separation. Therefore, ''separation of concerns'' achievement [12] gives way to ease process and decision model maintainability [13, 14].

Several research works and approaches have treated the integration of DMN decision models as complementary models to the BPMN business process models with the aim separating concerns for modelling care pathway processes. In [15], the BPMN and DMN are used to model and standardize the processes and decisions involved in initiating birth control. The presented model could be incorporated into an electronic health records system or health information systems. The paper [16] considers the extraction of DMN decision models from BPMN process models. It focuses on the data perspective of process models and provides an approach to derive a DMN model including decisions. In [13], a semi-automatic approach is introduced to identify decision logic in process models, to derive a corresponding DMN model and to adapt the original process model by replacing the decision logic accordingly, and to allow final configurations of this result during post-processing. Based on comparing the standard BPMN approach with the combination of both BPMN and DMN, the paper [4] examines the modelling of IoT processes. In [17], the paper describes the novelties introduced in a clinical decision support system capable of visualizing guideline progress and of supporting clinical decisions in the context of antimicrobial stewardship programs.

Current researches do not consider decisions about the sensitive data protection while the care pathways' business processes are rolling on. Such data should be protected in compliance with personal data protection laws and legislation, as the mentioned above. Therefore, protection requirements should be integrated in care pathways models for feature implementation in Hospital Information Systems. This could be insured only by modelling data-driven and privacy-oriented care pathways. In this context, we present, in this paper, an approach for modelling care pathway using BPMN combined with DMN in order to integrate decisions about the personal data protection in compliance with the security and privacy requirements particularly of legal aspect. HIPAA.

3. HIPAA requirements for protecting personal data

The HIPAA (Health Insurance Portability and Accountability Act) legislation helps to assist healthcare organization and providers in recognizing the flow of healthcare information. It describes how sensitive medical data should be protected from stealing and tampering [1]. HIPAA covers three main entities: (1) Healthcare service providers as doctors and the clinical staff, (2) healthcare plan providers as the insurance partners and (3) healthcare clearinghouses as the billing services and the repricing companies [18]. HIPAA laws identify 18 data as individually identifiable health information which are illustrated in a previous work [19].

In this work, we are highlighting the HIPAA privacy requirements for two main purposes of the sensitive medical data usage:

- Managing medical data for primary use such as direct care, treatment and payment.
- Managing medical data for secondary use as the public health and the public research.

Therefore, the DMN is used to take decision about the data privileges of access and the protecting methods. All this will be described in details in the following section.

4. Material and methods

In this paper, we are proposing a data protection process management in order to protect the patients' sensitive data in its standardized structure CDA documents which is defined by the HL7 standard. Our approach is based on filtering medical data processed throughout the care pathways rolling out. The filtering step could be applied according to user's role, the data context of use and the data type. Hence, we are aiming to implement the privacy management process with the executed care pathway processes. The privacy process offers a run time data transformation at the presentation level on the GUI interface.

5. Use case: sensitive data protection in medical imaging using BPMN decision modelling

The purpose of this section is to report our case study and to detail our approach. We consider the protection of sensitive medical data used for both primary and secondary use as our first concern. We are choosing to focus on one of the clinical pathways that is common to many healthcare services usually invoked as part of various care pathways such as cancer and covid-19 diagnosis processes.

5.1. BPMN model of the Imaging process

Before getting to grips with the proposed data protection process model, we studied, as a first step, the different tasks, activities, participants and information handling interactions executed as part of the imaging process. This is a very important step to be able to illustrate the utility of our security model and approach which allows to enforce the security measures of the sensitive health information. The radiological imaging process for oncological diagnosis usually is a complex process from requesting an exam to its undertaking and images visualization. Planning a radiological exam combines various types of integrated systems. It gathers diverse data coming from the involved healthcare information systems. It generates itself also many information in various formats: HL7 messages, text documents in the form of CDA, DICOM images, Structured reports and other types of data not directly related to the patient.

To better govern the use of the sensitive aspect of the shared medical data, it is important to discover them in the form of inputs and outputs of the different activities and tasks which are depicting the imaging process. A handy way to do this is through modelling care pathways in the form of business process models following the standard notation BPMN 2.0. This standard allows to extend the human and the systems interactions' definition and to refine events' composition and correlation. In addition, it allows to formalize the execution semantics for all the defined elements. It distinguishes between Flow Objects, Data Elements and Artifacts which offers a transparent presentation of processes [20].

The illustrated BPMN imaging process model in Fig.1 presents the shared and the managed medical documents and data between health care providers which are electronically transmitted between Hospital Information Systems. As presented in the imaging process, patient information is processed throughout tasks such as requesting radiology exams, assigning appointments, taking images and visualizing medical images. This helps to define the participants' role during the course of tasks and events. As well as, it helps to highlight the shared data.

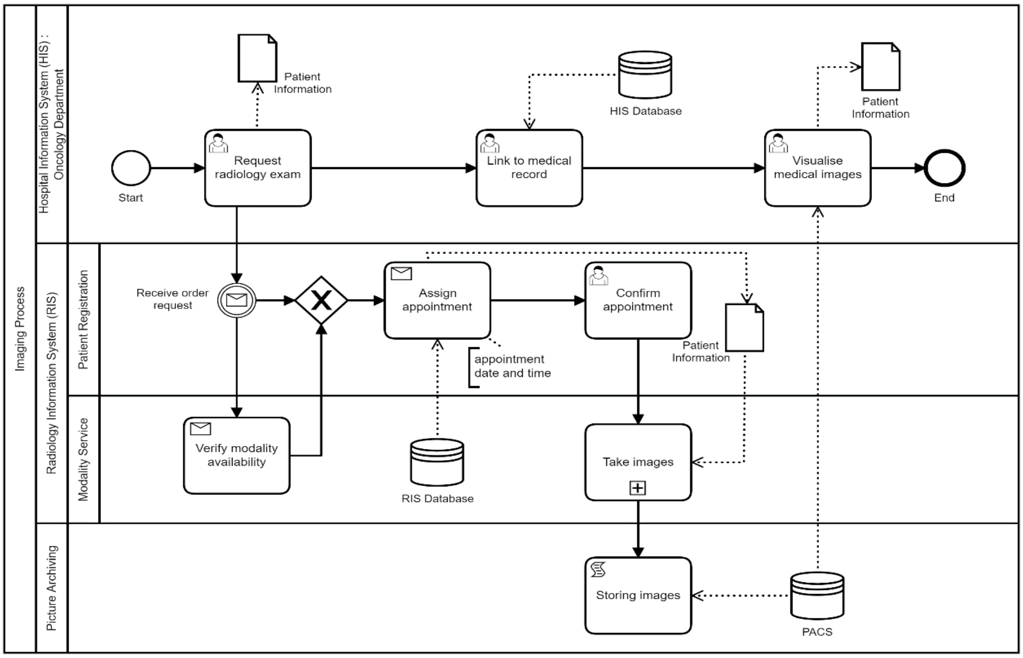


Fig. 1: The medical imaging care pathway BPMN model

5.2. BPMN/DMN model of medical document protection process

The security enhancement of sensitive data protection enforces the security layer of the involved systems in managing medical data. Therefore, we propose medical document process management offering an enforced protection of sensitive personal data included in shared ones as illustrated in Fig.2. The involved Hospital Information systems in processing data are allowed to be accessible throughout the user authentication. This enables the platform to open a specific session to each user with the permitted privilege of access. So, each user has predefined role with possible purposes of use of the managed medical documents. According to the user profile, the process will decide about the possible contexts of data usage. After choosing the medical document that would be disclosure, the user is permitted to choose one of the allowed purposes of use. Then the sub-process “manage protection” will take place allowing to apply the appropriate protection method. Finally, the sensitive data will be showed in a protected form and the HIPAA requirements will be displayed.

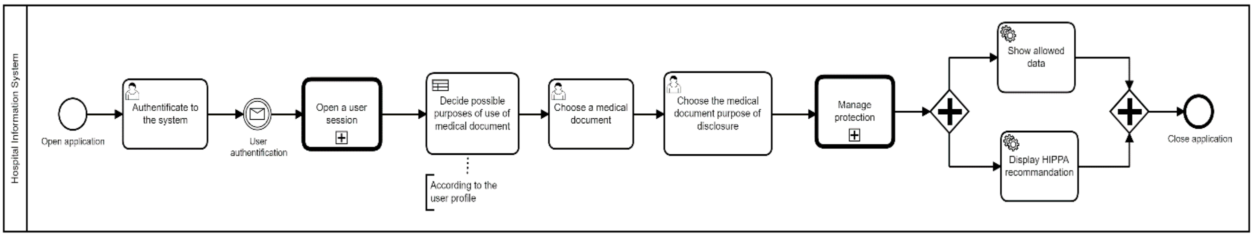
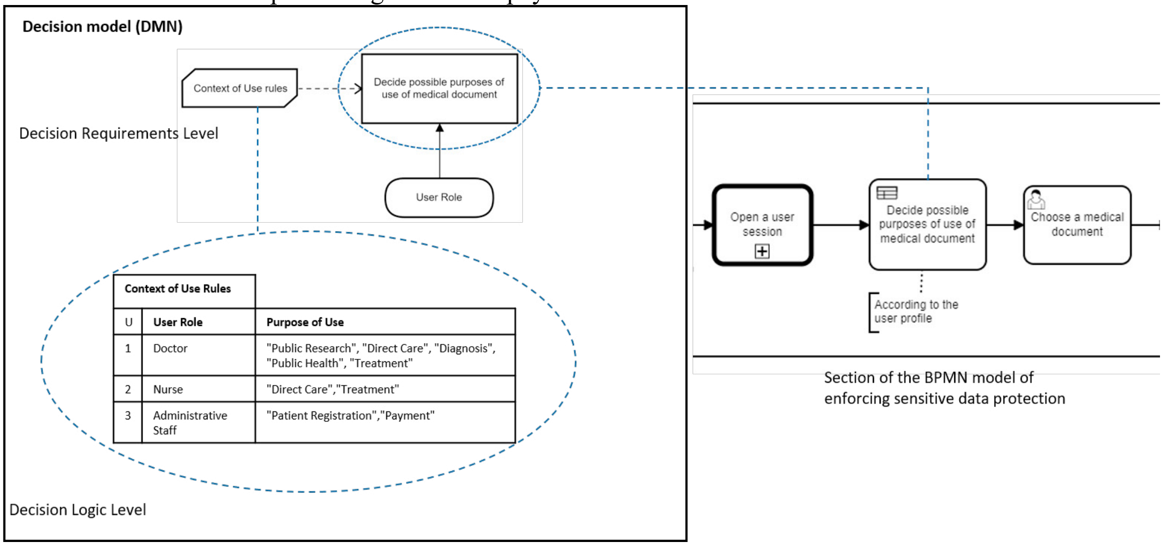

Hospital Information System
Open application
Authentificate to the system
User authentification
Open a user session
Decide possible purposes of use of medical document
According to the user profile
Choose a medical document
Choose the medical document purpose of disclosure
Manage protection
Show allowed data
Display HIPPA recommandation
Close application

Fig. 2: BPMN model for enforcing sensitive data protection

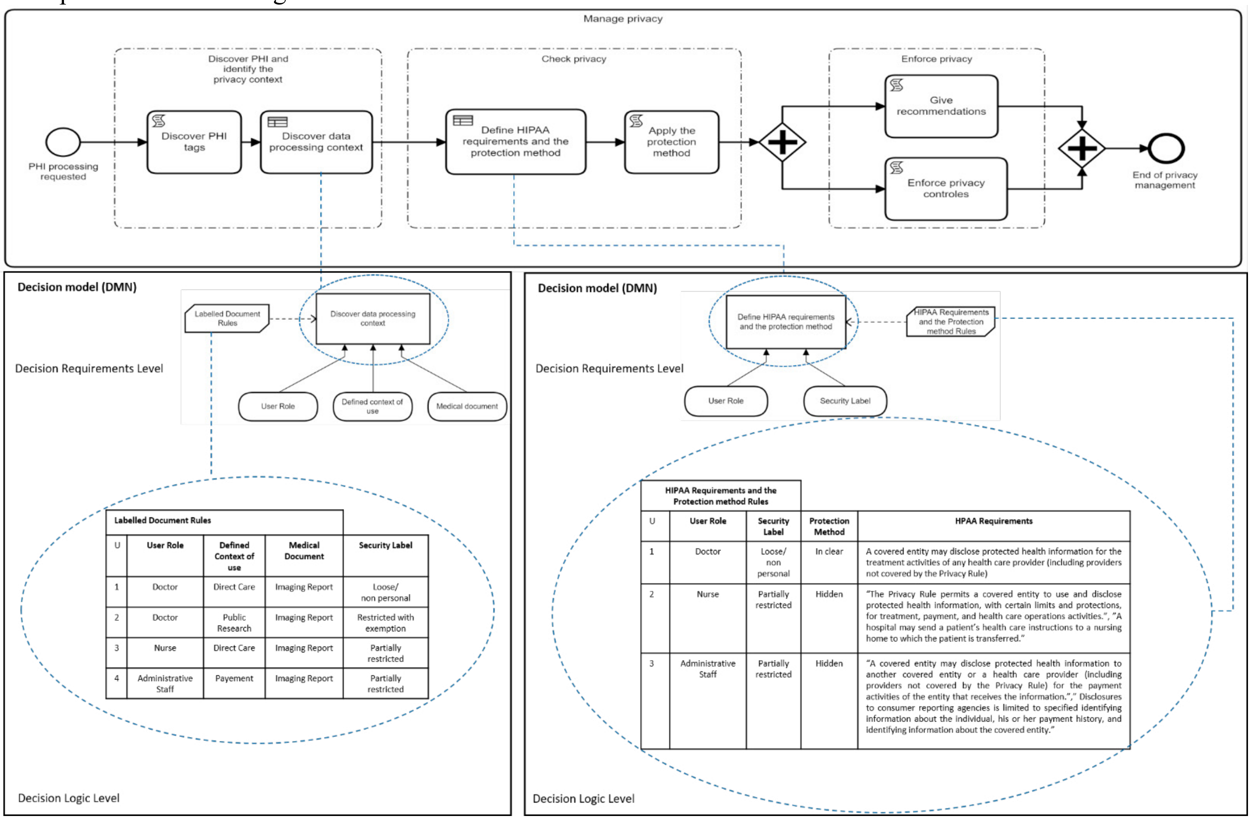
After defining the user role, each user has asset of allowed context of use of the medical documents. As presented in the Fig.3, if the user is a doctor, then he/she is allowed to use the medical documents for several purposes as the direct care, the diagnosis, the treatment, the public research and the public health. If the user is a nurse, then he/she could use the medical data for the direct care or the treatment purposes. Contrary to the administrative staff who could only use the medical data for patient registration or payment.


Decision model (DMN)
Context of Use rules
Decide possible purposes of use of medical document
Decision Requirements Level
User Role
Decision Logic Level
Open a user session
Decide possible purposes of use of medical document
Choose a medical document
According to the user profile
Section of the BPMN model of enforcing sensitive data protection

Context of Use Rules		
U	User Role	Purpose of Use
1	Doctor	"Public Research", "Direct Care", "Diagnosis", "Public Health", "Treatment"
2	Nurse	"Direct Care","Treatment"
3	Administrative Staff	"Patient Registration","Payment"

Fig. 3: BPMN/DMN modelling of possible data context of use for each user role

The security enforcement is insured by the sub-process "Manage privacy". This sub-process is divided into three main parts as shown in Fig.4.


Manage privacy
Discover PHI and identify the privacy context
Check privacy
Enforce privacy
PHI processing requested
Discover PHI tags
Discover data processing context
Define HIPAA requirements and the protection method
Apply the protection method
Give recommendations
Enforce privacy controles
End of privacy management
Decision model (DMN)
Labelled Document Rules
Discover data processing context
Decision Requirements Level
User Role
Defined context of use
Medical document
Decision Logic Level
Decision model (DMN)
Define HIPAA requirements and the protection method
HIPAA Requirements and the Protection method Rules
Decision Requirements Level
User Role
Security Label
Decision Logic Level

Labelled Document Rules				
U	User Role	Defined Context of use	Medical Document	Security Label
1	Doctor	Direct Care	Imaging Report	Loose/ non personal
2	Doctor	Public Research	Imaging Report	Restricted with exemption
3	Nurse	Direct Care	Imaging Report	Partially restricted
4	Administrative Staff	Payement	Imaging Report	Partially restricted

HIPAA Requirements and the Protection method Rules				
U	User Role	Security Label	Protection Method	HPAA Requirements
1	Doctor	Loose/ non personal	In clear	A covered entity may disclose protected health information for the treatment activities of any health care provider (including providers not covered by the Privacy Rule)
2	Nurse	Partially restricted	Hidden	"The Privacy Rule permits a covered entity to use and disclose protected health information, with certain limits and protections, for treatment, payment, and health care operations activities.", "A hospital may send a patient's health care instructions to a nursing home to which the patient is transferred."
3	Administrative Staff	Partially restricted	Hidden	"A covered entity may disclose protected health information to another covered entity or a health care provider (including providers not covered by the Privacy Rule) for the payment activities of the entity that receives the information."," Disclosures to consumer reporting agencies is limited to specified identifying information about the individual, his or her payment history, and identifying information about the covered entity."

Fig. 4: BPMN/DMN model for managing the medical document privacy

The first part concerns PHI (Protected Health Information) discovering and privacy context identifying. The PHI discovering could happen by the use of a script activity which allow to identify the eighteen PHI defined in the HIPAA rules. Then the decision activity of discovering data processing context consists in making decision about labelling the chosen medical document which is used in a standardized form as CDA-HL7 and DICOM. This needs the definition of the user role and the context of use of the medical data and the chosen medical document. As a consequence, the outcome of this task is a labelled copy of the medical document. For the same user, the medical document could be labelled differently depending on the context of use. In the second part, the process will check the privacy by defining the HIPAA privacy requirements and the required protection method according to the user role and the affected security label to the medical document. Then, a script activity will be in charge of applying the relevant protection method to the labelled medical document. the third part is responsible of enforcing the privacy by executing two parallel script activities allowing to give and display the HIPAA recommendations and to enforce privacy controls by displaying the medical document in a protected form. This privacy management system could be integrated and deployed in the HIS. This will act as a privacy booster to the security layer of the system and invoked every time when patient data are being processed. In the example of the imaging care pathway, the manage privacy sub-process could be integrated while retrieving patient data from the RIS (Radiology Information System) Database for assigning appointment, transferring patient data to take images and retrieving medical images from the PACS (Picture Archiving and Communication System) for visualization.

6. Results and discussion

In this work, we aimed to enhance the enforcement of sensitive data protection while processing medical documents using Hospital Information Systems. The security of patient data has become a challenging issue held into consideration by the personal data protection laws. Therefore, we propose an approach which is based on an illustration of HIPAA compliant privacy management processes. These processes are combined with care pathways business processes to add security and privacy consideration while processing patient data for several purposes of use. These data should be protected according to the purpose of use of the medical document in which they are included and according to the healthcare provider's role by implementing computerized data protection methods. Each medical document could be protected with a specific protection method according to its type and the attributed security label.

Our security approach is based on decision making features that are complementary to business process modeling. This has particularly allowed to determine the level of security each medical data/document requires. Since the BPMN models lacks the capability for representing decisions, we have used DMN decision tables to model BPMN decision as aggregated processes. In this way, we managed to present both the activity or the task requiring a decision and the logics of the applicable DMN decision models. The BPMN models defines tasks within business processes where decision-making is required to occur. The decision requirements level is forming a bridge between business process models. It defines the decisions to be made in business processes' tasks, their interrelationships, and their requirements for decision logic. As for the decision logic level, it serves to define the required decisions in sufficient detail to allow validation and/or automation. Our approach allows the enforcement of the security layer of the Hospital Information Systems in compliance with HIPAA security requirements.

7. Conclusion

Integrating computerized systems in healthcare environment although their evidenced benefits present high risk for illegal disclosure of sensitive medical data. At the same time imposing overly fenced controls could affect patient's life who is the subject of the shared medical documents. Hence, patient security and privacy has become one of the main concerns in the medical field. Unfortunately, personal data protection law such as HIPAA and GDPR requires the adoption of a complexes and difficult to implement legal frameworks to preserve in a balanced way, the patient confidentiality and to allow the smooth running of healthcare operations. In this work we have tried to simplify the implementation of these legal requirements but correlating privacy compliance measurements with clinical business processes.

Based on the HIPAA Privacy Rule requirements and the BPMN standard, we proposed a privacy enforcing approach. Our approach is based on leveraging a seamless way for the decision making about the security level the data requires. It implements the BPMN privacy decision processes. This allows to model the process level using BPMN models combined with the DMN for integrated decision making as business logic requirements. We rely on the use of fine-grained security and privacy labels of the date to be able to work out the right decision described in the DMN of each process. Our approach seems to have a very good impact on enhancing and enforcing the security layer of the Hospital Information Systems in compliance with HIPAA security requirements. In addition, this approach could be adapted to any care pathway and to diverse legal frameworks protecting personal data. It could be also adopted to develop a privacy by design approach when designing hospital information systems.

In future work, we are aiming to propose an approach to estimate and evaluate the privacy risks and non-compliance of hospital information systems. This could help healthcare organization to assess the privacy and security level of the existing systems and integrate the required measures and safeguards to manage their care pathways.

References

[1] Patil A P and Chakrabarti N 2021 A review into the evolution of HIPAA in response to evolving technological environments Journal of Cybersecurity and Information Management 4 5--15

[2] Looten V and Simon M 2020 Digital Personalized Health and Medicine: IOS Press) pp 1133-7

[3] Νούσιας N 2021 Business process and decision automation: end-to-end deployment with a BPMN and DMN-based workflow engine

[4] Hasić F, Serral E and Snoeck M 2020 Comparing BPMN to BPMN+ DMN for IoT process modelling: a case-based inquiry. In: Proceedings of the 35th Annual ACM Symposium on Applied Computing, pp 53-60

[5] (2015) O M G 2021 Decision Model and Notation. Version 1.3

[6] Buzink S N, van Lier L, de Hingh I H and Jakimowicz J J 2010 Risk-sensitive events during laparoscopic cholecystectomy: the influence of the integrated operating room and a preoperative checklist tool Surgical endoscopy 24 1990-5

[7] McLachlan S, Kyrimi E, Dube K, Hitman G, Simmonds J and Fenton N 2020 Towards standardisation of evidence-based clinical care process specifications Health informatics journal 26 2512-37

[8] Pedersen K Z and Obling A R 2020 'It's all about time': Temporal effects of cancer pathway introduction in treatment and care Social Science & Medicine 246 112786

[9] Braun R, Schlieter H, Burwitz M and Esswein W 2015 Extending a Business Process Modeling Language for Domain-Specific Adaptation in Healthcare. In: Wirtschaftsinformatik, pp 468-81

[10] Bazhenova E and Weske M 2016 Deriving decision models from process models by enhanced decision mining. In: International conference on business process management: Springer) pp 444-57

[11] Wiemuth M, Junger D, Leitritz M, Neumann J, Neumuth T and Burgert O 2017 Application fields for the new object management group (OMG) standards case management model and notation (CMMN) and decision management notation (DMN) in the perioperative field International journal of computer assisted radiology and surgery 12 1439-49

[12] Parnas D L 2002 Software pioneers: Springer) pp 411-27

[13] Batoulis K, Meyer A, Bazhenova E, Decker G and Weske M 2015 Extracting decision logic from process models. In: International conference on advanced information systems engineering: Springer) pp 349-66

[14] Hasić F, De Smedt J and Vanthienen J 2018 Augmenting processes with decision intelligence: Principles for integrated modelling Decision Support Systems 107 1-12

[15] Sooter L J, Hasley S, Lario R, Rubin K S and Hasić F 2019 Modeling a Clinical Pathway for Contraception Applied clinical informatics 10 935-43

[16] Bazhenova E, Zerbato F, Oliboni B and Weske M 2019 From BPMN process models to DMN decision models Information Systems 83 69-88

[17] Cánovas-Segura B, Zerbato F, Oliboni B, Combi C, Campos M, Morales A, Juarez J M, Marin R and Palacios F 2017 A process-oriented approach for supporting clinical decisions for infection management. In: 2017 IEEE International Conference on Healthcare Informatics (ICHI): IEEE) pp 91-100

[18] Assistance H C 2003 Summary of the hipaa privacy rule Office for Civil Rights

[19] Intidhar E, Hanene B R and Mohamed Fethi L 2019 Sensitive Data Discovery in Care Pathways using Business Process Modelling and HL7-CDA International Journal on Advances in Life Sciences 11 56-67

[20] Dijkman R, Hofstetter J and Koehler J 2011 Business Process Model and Notation vol 89: Springer)