Data Driven Medical Process Modelling for Privacy Protection in Care Pathways

Intidhar Essefi
University of Tunis el Manar, The Higher Institute of Medical Technologies of Tunis
Research Laboratory of Biophysics and Medical Technologies
Tunis, Tunisia
e-mail: essefi.intidhar@gmail.com

Hanen Boussi Rahmouni
University of Carthage,
Higher School of Communication of Tunis
Digital Security Research Unit
and
University of Tunis el Manar, The Higher Institute of Medical Technologies of Tunis
Tunis, Tunisia
e-mail: hanene.boussi@istmt.utm.tn

Mohamed Fethi Ladeb
Radiology Department
Kassab Orthopedics Institute
Manouba, Tunisia
e-mail: fethiladeb@hotmail.fr

***Abstract*—In this article, we present a clinical pathway specification methodology for data driven medical process modelling. Our model takes into consideration patients privacy preservation. It gives special attention to shared medical documents structure and content. Furthermore, our model describes the different clinical tasks, typically included in hospitals care pathways. It also exposes the underlying shared patient data enclosed within the medical documents required by the clinical pathway subject to execution. This research aims first of all to identify, for each clinical task that requires data processing or sharing, the level of protection that data requires. For this, we suggest to extend existing business process modelling languages with special means highlighting medical data. As a second step, we aim to map each extracted data category to a set of privacy requirements as demanded by the Health Insurance and Accountability Act (HIPAA) legislation. This will ensure the respect of data protection requirements since a very early stage of Hospital Information Systems (HIS) design.**

Keywords-business process modelling; clinical pathways; data driven; HIPAA legislation; patient privacy; privacy requirements.

I. INTRODUCTION

In order to improve services' quality within a hospital environment, it is important to automate the underlining workflows of each clinical process adopted within the hospital. This needs the design and the implementation of business process models tailored for the concerned field. Medical healthcare is a multidisciplinary field. Its business processes and workflows are very complex. Throughout each medical process, several types of clinical information need to be circulated and treated within or without the hospital's boundaries. Medical data are produced, transmitted between medical departments and shared between healthcare professionals throughout the clinical pathways enforced by the hospital information systems in use. Several types of medical data documents are processed, including admission papers, insurance documents, prescriptions, confidential letters, medical images, imaging reports, biological reports, other types of medical reports, etc. All the mentioned clinical documents include diverse health information, among which we distinguish sensitive information that is considered as highly Protected Health Information (PHI). Personal healthcare information is not only used in healthcare practices and shared between healthcare professionals, but also in public practices and research activities such as public health surveillance and public health research. Public health practices and research present risks that are related to the unauthorized disclosure of PHI [1]. Therefore, it is crucial for healthcare organizations to ensure PHI protection and to preserve the privacy of individuals. Particularly, the individual's privacy protection is required by legislation, such as the Health Insurance Portability and Accountability Act (HIPAA) legislation [16][17] and the European Directive [18] on personal data protection. As a consequence, privacy requirements should be respected and ensured when designing systems and procedures for health data management.

Our approach is based on privacy by design, which means the implementation of privacy requirements since an early stage of healthcare information systems design with respect to carrying out clinical pathways. In this paper, we take the osteosarcoma clinical pathway as a case study to validate our approach. The details of our approach are as follows:

- Model medical care pathways as business processes that emphasise shared clinical data aiming to identify sensitive health information among them.
- Identify the privacy requirements and procedures for each type of sensitive health data identified within the business process representing each care pathway.
- Identify a clinical data model based on the business process modelling.
- Define the sensitive health information categories.
- Define the HIPAA legislation requirements to preserve the patient's privacy and confidentiality with regards to the use of their PHI.
- Model the clinical pathways based on business process modelling in order to extract the shared clinical documents between healthcare professionals.
- Identify the PHI underlining each process model.

- Define privacy requirements for PHI protection from any disclosure or misuse.

This paper is divided into sections as follows: in Section II, we present the related work; in Section III, we present the clinical pathway subject to study, as well as the clinical pathway modelling language of our choice. We adopt a data driven business process clinical pathway modelling approach. In Section IV, we present our clinical document architecture. In Sections V and VI, we define the privacy requirements for PHI, followed by results and discussion. In Section VII, we present the conclusion and future work.

II. Related work

In the literature, clinical pathways are textually and medically described. Their business processes and workflows are mostly detailed by doctors using textual description of the sequenced tasks. Due to the technological revolution in the medical field that includes medical information systems, several methods and business process modelling languages have emerged. This includes the Integration DEFinition language (IDEF) (V.0 and V.3), the Unified Modelling Language (UML) V.2.0 and the Business Process Model and Notation language (BPMN). Most of these technologies were also used to model clinical pathways [2].

BPMN is the most widely used and accepted language in medical process modelling thanks to its simple and high-level process construction. Clinical pathways processes are known as complex. This needs a transparency of the whole process elements such as structures, participants, tasks, roles, etc. Modelling care pathways in the form of clinical processes is considered as a solution to overcome its complexity and define its requirements with regards to patients and health care professionals. Therefore, medical processes models should be simple, transparent and understandable as much as possible [3][4].

Despite the importance of business process modelling in clinical pathways and efforts for processes' automation, few works are dealing with care pathways' automation. Most of them are relying on a business process-based modelling approach. Besides, there is some suggested BPMN extension implementation such as the Clinical Pathway (CP) extension of the BPMN called BPMN4CP which proposes an ontology based- extension for e-health process management. Other existing research works offer clinical textual description of the care pathways processes. In addition, other works were interested in analyzing systems behavior throughout business process-based modelling using UML, particularly, UML class diagram [5]-[7].

However, less effort was made in investigating approaches for clinical data modelling with special interest in privacy preservation. In this context, our work is addressed to the respect of privacy requirements since a very early stage of HIS design in order to ensure a protected rolling of data driven business processes that are clinical pathway-oriented.

III. Clinical pathways

Clinical pathways are acknowledged as complex processes due to the diversity of the participating entities (e.g., healthcare professionals and medical service providers). Throughout the literature exploration of the clinical pathways' modelling and automation, we extracted the main phases underlining care pathway processes. A generic clinical pathway begins by an admission phase in which the patient is allowed to get access to the care establishments. This is usually followed by a diagnosis phase: that describes the visiting of the consulting doctor and having clinical diagnosis performed. The treatment phase should then occur: after identifying the pathology in the second phase, the treating doctor identifies the treatment protocol. This clinical pathway ends with the follow-up phase which allows the involved practitioner to monitor and evaluate the effectiveness of the prescribed treatment or to control the pathology progression [8].

The clinical pathway is a set of processes and sub-processes in which one or more healthcare professionals participate. The business process modelling of clinical pathways allows to identify the tasks, the participants and their roles in the care pathway proceeding. Even the shared data between healthcare professionals may also be modelled and identified among a clinical pathway-oriented business process [9].

In the following sections, we will detail the clinical care pathway of osteosarcoma and describe a step by step methodology to model our clinical business process.

A. An Overview of Osteosarcoma Clinical Pathways

Osteosarcoma is a bone cancer. It most commonly reaches those aged from 10 to 30. A great part of this affected population concerns teenagers. Each year, from 800 to 900 people are estimated to be diagnosed with osteosarcoma in the United States. Osteosarcomas are primary malignant bone tumors. They can be classified according to cells' behavior under the microscope as high, intermediate or low grade [10].

Osteosarcoma clinical care pathways are characterized by their complex and multidisciplinary procedures with their difficult management facts. By Ferrante [3], the osteosarcoma first diagnosis starts with symptoms appearances like bone pain or soreness, a felt mass through the skin, swelling and redness, etc. During the clinical pathway diagnosis phase, while an osteosarcoma is suspected, some standard imaging exams must be performed. Once the osteosarcoma is confirmed and its malignancy is not excluded, a biopsy should be performed allowing the cancer staging. As a final checkup step, several imaging exams are performed to verify the existence of metastases. A percentage of 85% indicates that the most common metastases appear in the lung whereas the bone is considered as the second most common site of distant disease [11].

The osteosarcoma checkup and grading steps allow the choice of the treatment procedure which includes chemotherapy, radiation therapy and surgery operation. The identification of the right therapy protocol is based on biological analyses. To verify and evaluate the treatment efficiency, the patient has to be periodically followed-up. This osteosarcoma clinical pathway follow-up step is based on the performing of imaging exams in addition to biological analyses as needed [11]-[13].

The complexity of the osteosarcoma clinical pathway business process is due to the collaboration between healthcare professionals from several medical departments. This process can not be accomplished without clinical data sharing and transmission. For that, it is necessary to respect the applicable data protection regulation.

B. *BPMN as Clinical Pathway Modelling Language*

To model clinical pathways, we used the BPMN as a modelling language. It is the most widely used language in healthcare business process modelling. First, we explored the clinical healthcare pathways in the literature on description of clinical pathways. Then, we divided them into three main phases, diagnosis or check-up, treatment and follow-up, mentioned above. Throughout the studied clinical pathways, we present the osteosarcoma clinical pathway as a case study to illustrate our data driven clinical healthcare pathway model. In order to elaborate the clinical pathway data driven model, we used the common patterns and symbols of the BPMN modelling language [2].

C. *Osteosarcoma Clinical Pathway Modelling Using BPMN*

In order to identify the clinical data that may be transmitted and shared between healthcare professionals as required by standard care pathway specifications, we modelled the osteosarcoma clinical pathway in the form of a business process model. In this way, we could first identify the characteristics of performed clinical tasks. Then, we could highlight the data driven tasks for the chosen pathology. The sections below present the data driven clinical pathways of osteosarcoma for the check-up, the treatment and the follow-up phases respectively.

1) *Osteosarcoma checkup clinical pathway*

Fig. 1 presents the check-up phase of the osteosarcoma clinical pathway as well as the shared and transmitted clinical documents, ensuring the steps required by the care pathway definition. The osteosarcoma clinical pathway is complex and involves collaboration of healthcare providers and diverse medical services including radiology, biology, nuclear medicine, surgical units, etc., as shown in Fig. 1, Fig. 2 and Fig. 3. After the patient admission, a medical consultation takes place. According to the clinical examination, medical tests are performed to accomplish the diagnoses phase and precise the pathology Fig. 1.

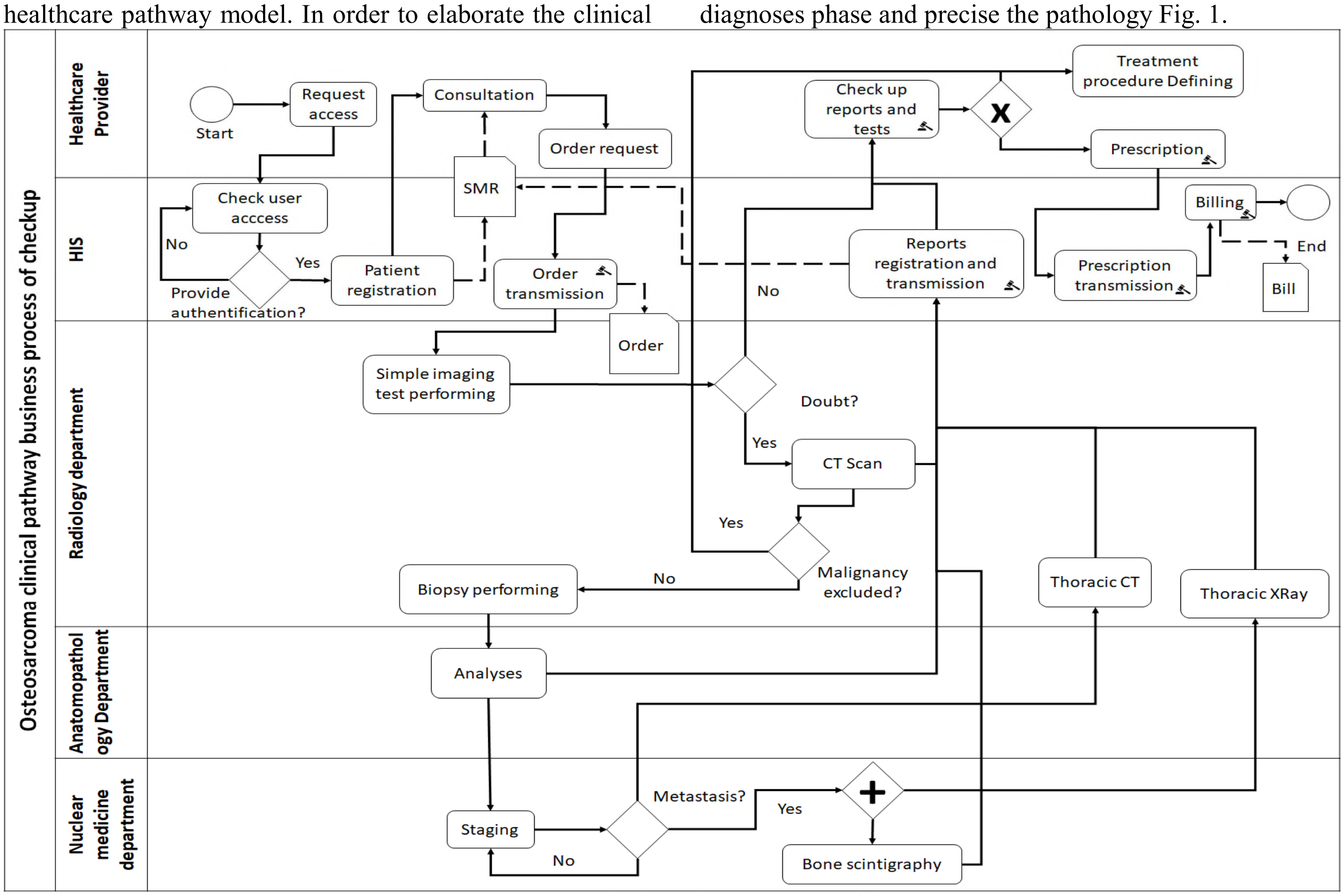

Figure 1. Osteosarcoma clinical pathway business process of checkup.

2) Osteosarcoma treatment clinical pathway

Based on tests' findings within the diagnosis phase, the doctor defines the treatment phase according to systems review by biological tests, audiogram hearing tests and heart tests. By Luetke [12], during the treatment, medical tests and clinical examination are performed to evaluate its effectiveness, as shown in Fig. 2.

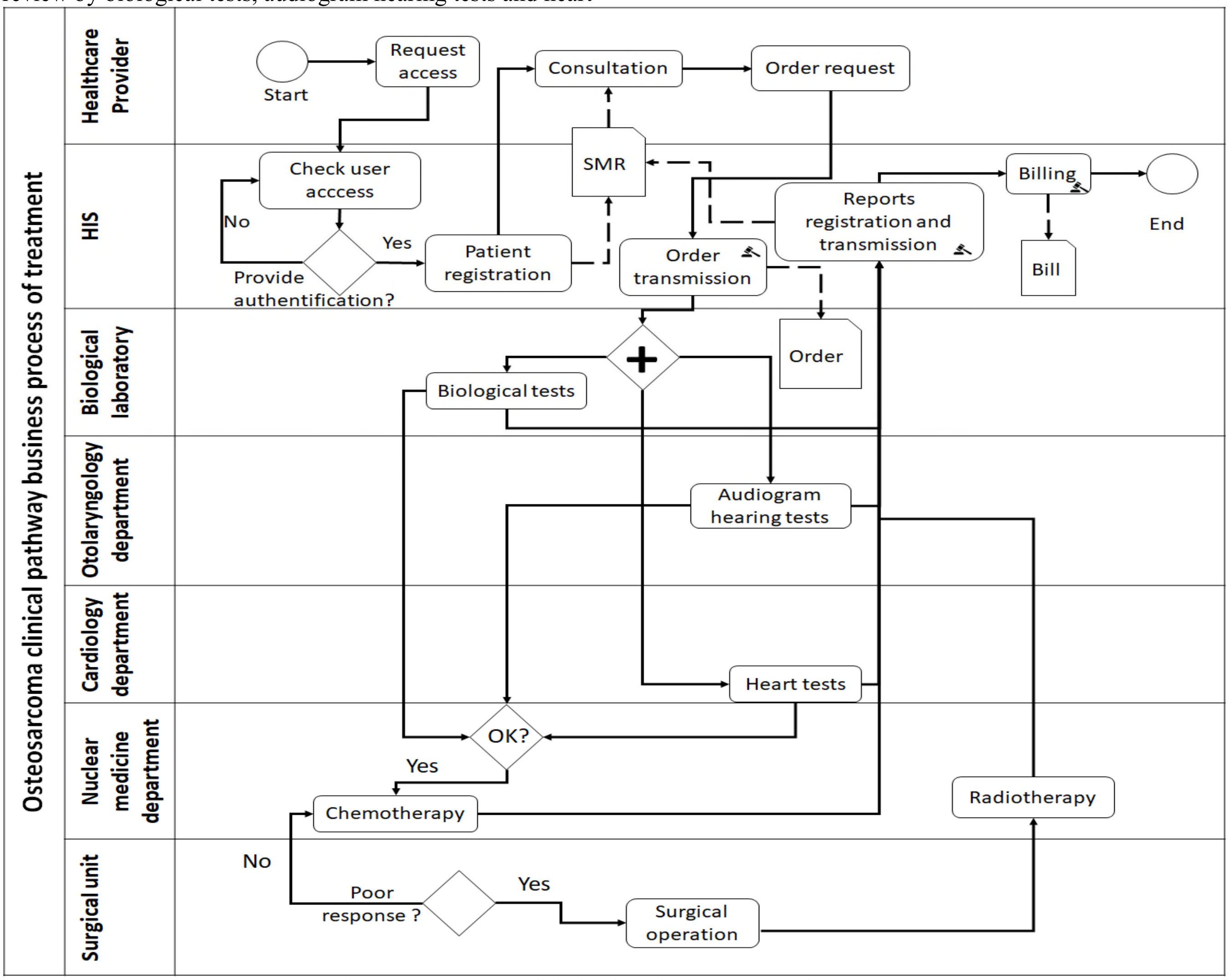

Figure 2. Osteosarcoma clinical pathway business process of treatment.

3) Osteosarcoma follow up clinical pathway

The last step is the following-up phase presented in Fig. 3. According to Paiolil [13], the doctor follows the patient health status by performing some tests and medical examination to check periodically the treatment effectiveness. Throughout the three phases of the osteosarcoma clinical pathway, diverse clinical documents are shared, transmitted and updated within the Shared Medical Record (SMR) ensuring the healthcare continuity.

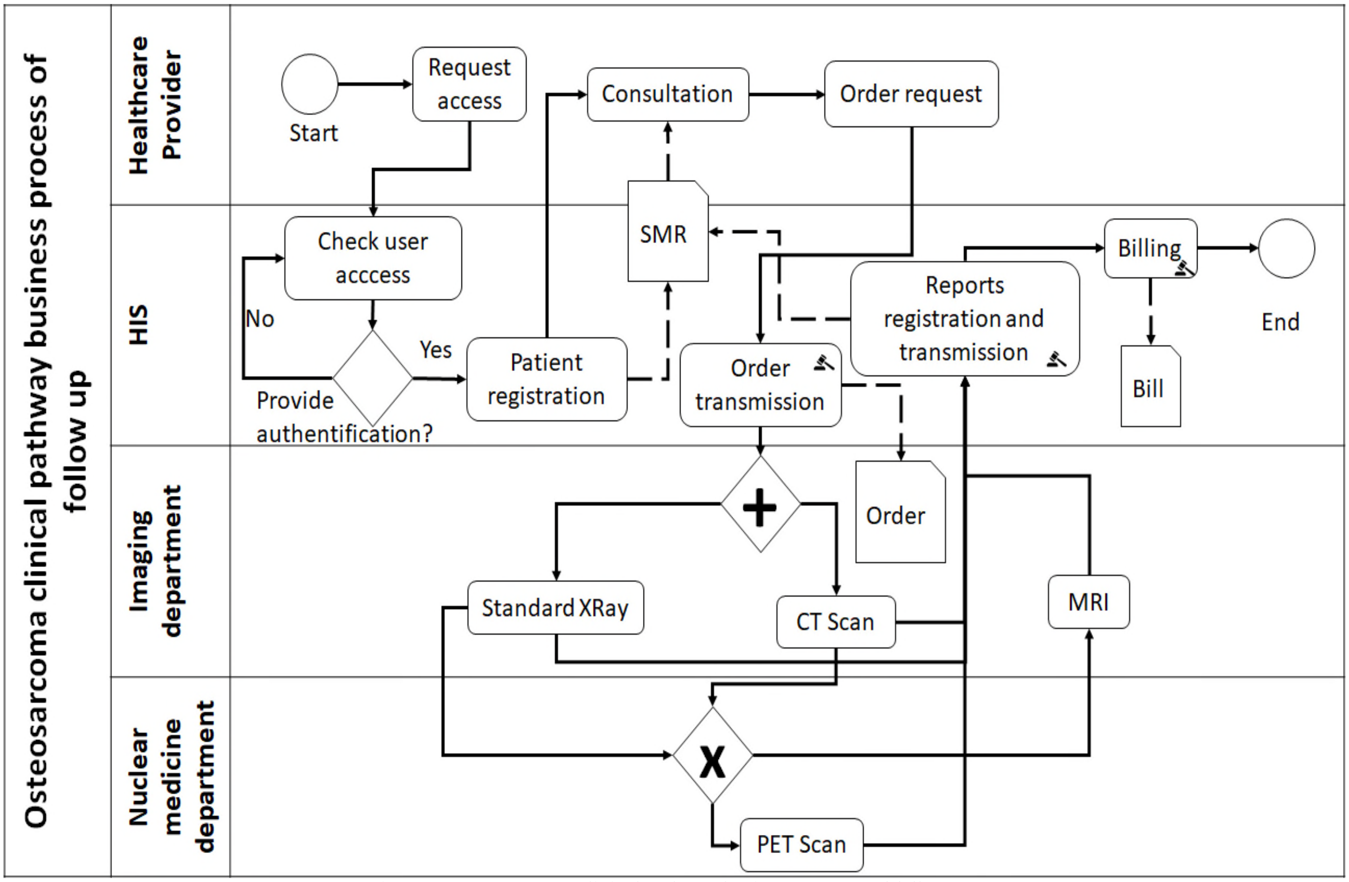

Figure 3. Osteosarcoma clinical pathway business process of follow up.

IV. SHARED CLINICAL DOCUMENT ARCHITECTURE

A patient's Electronic Health Record (EHR) must contain all types of clinical documents including their medical history record, discharge summaries, typical paper charts, mental status examinations and other medical reports, such as medical tests and operative reports.

Throughout a clinical business process, the EHR is transferred, updated and shared between healthcare professionals ensuring the continuity of care. Each clinical document included in the EHR contains medical data as it is required in the concerned healthcare establishment.

The general clinical document architecture is divided into documents, fragments and data. As shown in Fig. 4, clinical documents are composed of many fragments. They provide information about patients, procedures, practitioners, diagnosis, findings and appointments. The clinical shared documents' architecture model, illustrated in Fig. 4, could be adapted to another health care establishment, according to the used medical documents' structure in their boundaries. In each clinical document fragment, several medical data are found with specific properties which need the implementation of a privacy by design approach. This is dedicated to the PHI use and disclosure within the HIS. The identification and demographic fragments in clinical documents include PHI. Its use should obey to the data protection law principles and privacy requirements ensuring the PHI privacy and the security of the medical data in use [14] [15].

This could be applied by the use of security computerized methods (e.g. encryption, decryption, anonymization and pseudonymization) since an early stage of the design of the HIS.

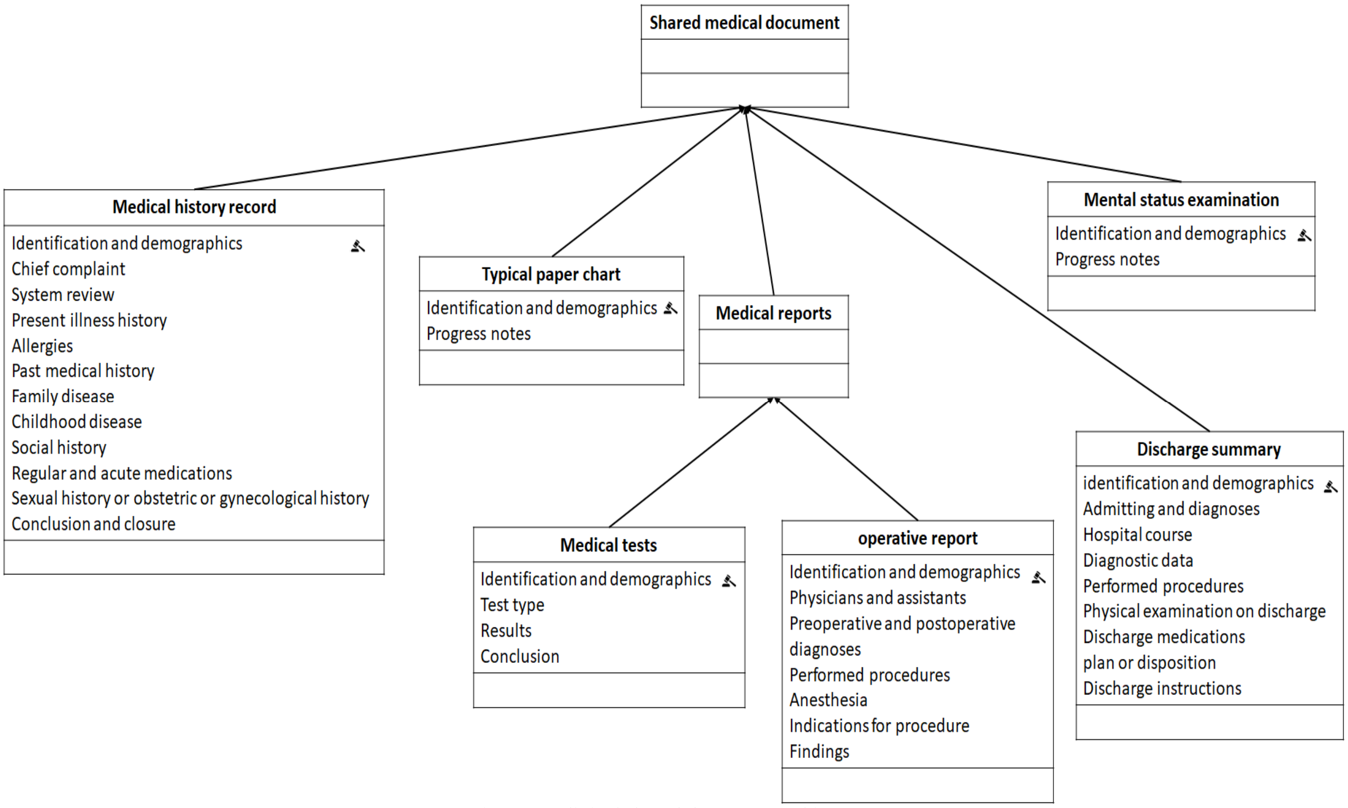

Figure 4. Clinical shared document architecture.

V. PRIVACY REQUIREMENTS FOR PHI PROTECTION

The use of clinical healthcare data is governed by many jurisdictions as it may present risks threatening a person's life and may affect both his privacy as well as his professional life. For this, Clinical data usage must be set for data protection principles. In particular, the following eight principles should be respected:

1- Lawfulness, fairness and transparency: personal data should be processed lawfully, fairly in a transparent way.
2- Purpose limitation: personal data should be processed for specific purposes.
3- Data minimization: personal data should be adequate, relevant and limited to the precise purposes.
4- Accuracy: personal data should be kept up to date.
5- Storage limitation: personal data should be kept for no longer than the necessary period for the purposes for which those data are processed.
6- Rights: people have the right to access their data and give permission for other entities to use or disclose them.
7- Integrity and confidentiality: personal data should be processed in a secure way. They should be protected also against any unauthorized or unlawful processing, accidental loss, destruction or damage.
8- International transfers: personal data should not be transferred outside countries [14].

International law frameworks, such as European directive and HIPPA for personal data protection are based on the previous data protection principles. The present work is developed with regard to Protected Health Information within HIPAA regulation. The HIPAA Privacy Rule is published by the department of Health and Human Services (HHS) to ensure health information privacy. The privacy rule is applied to covered entities as health plans, healthcare clearinghouses and the healthcare providers. It defines a set of rules in order to protect sensitive health information with respect to its use and disclosure. Sensitive health information is known as Protected Health Information (PHI). They are individually identifiable health information related to the patient's past, present and future physical or mental health conditions, the healthcare provision to the individuals and the past, present or future healthcare provision to individuals [1]. The individually identifiable health information includes demographic data and many common identifiers. PHI usage and disclosure are permitted without the patient's informed consent for some purposes and situations as to the individual, the treatment, payment and healthcare operations, opportunity to agree or object, incidence to an otherwise permitted use and disclosure or public interest and benefit activities as well as a limited data set for research, public health or healthcare operations purposes or when it is required by law. As for the not

 ISBN: 978-1-61208-682-8

permitted PHI usage and disclosures, an individual's written authorization (consent) must be obtained [16].

In addition to permitted PHI use and disclosure, prohibited ones are defined in Privacy Rules. For example, genetic information is considered as PHI and they shall not be used or disclosed for underwriting purposes as well as the psychotherapy notes. Furthermore, PHI may not be sold by covered entities. The PHI use and disclosure must be limited to the minimum necessary. However, PHI may be used to create a non-individually identifiable health information or a de-identified information [16][17].

The HIPAA Privacy Rule also defines a set of PHI de-identification requirements in order to use and disclose it without the patient's authorization. A covered entity may de-identify PHI by removing the eighteen identifiers specified in the following list:

1. Names.
2. Addresses with all geographic subdivisions smaller than a State.
3. Dates except year (birthdate, admission and discharge date, date of death).
4. Telephone numbers.
5. Fax numbers.
6. Email addresses.
7. Social security numbers.
8. Medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
11. Certificate/license numbers.
12. Vehicle identifiers, serial numbers and license plate numbers.
13. Device identifiers and serial numbers.
14. URLs (Web Universal Resource Locators.
15. IP (Internet Protocol) address numbers.
16. Biometric identifiers (finger and voice prints).
17. Full face photographic images and any comparable images.
18. Any unique identifying number characteristic or code [16].

For the above identified PHI use and disclosure purposes, de-identification based on computerized methods is necessary to respect the PHI privacy and ensure its protection from any illegal use or other threatening risks.

VI. RESULTS AND DISCUSSION

In this present work, we are interested in studying medical business processes in order to elaborate a data driven clinical pathway model, based on the BPMN language. The aim here is to ensure the respect privacy requirements since early stages of HIS design. Then, we divided clinical data into categories and extracted PHI among them in the form of data model clinical pathway. After that, we defined both personal data protection principles and HIPAA privacy requirements for the specified PHI use and disclosure. Finally, all of the above listed objectives were validated through the modelling of osteosarcoma care pathway business process model chosen as a case study.

As for the completion of the modelling phase of osteosarcoma clinical pathway, we have modeled its complex care pathway which is divided into three phases: *check-up*, *treatment* and *follow-up.* This was done using the actual BPMN language simple patterns. Hence, personal data processing is integrated in the processes, particularly, in a legislation compliant manner which adds more trust to medical documents processing and sharing during the clinical process implementation.

Many difficulties were encountered in clinical pathway modelling using BPMN due to the complexity and multidisciplinary aspect of medical procedures. This has led us to conclude the necessity of a more specialized care pathway modelling language. This has also highlighted the need for a new care pathway modelling and automation language that is sensitive-data driven and could integrate privacy requirements specification. Thus, a new extension of the BPMN modelling language is required.

VII. CONCLUSION AND FUTURE WORK

Clinical pathways automation is highly required in standardized HIS. This is traditionally ensured by business process modelling. In this context, we developed a data driven clinical pathway business process model for osteosarcoma, as a case study. We used BPMN as clinical pathway business process modelling language. A shared clinical data model was elaborated further to the clinical business process model.

Since personal data management must obey to data protection law, we defined both personal data protection principles and HIPAA privacy requirements with relation to patients identifying medical documents, in terms of their both use and disclosure.

The adoption of a privacy by design approach offers a better enforcement of privacy since an early stage of computer-based healthcare systems design. This allows an orthogonal integration of privacy obligations throughout the clinical process. For this reason, we are working currently on extending the BPMN process modelling language with privacy annotation features and additional patterns to allow the modelling of privacy specification as part of clinical processes.

We are aiming to define a common vocabulary qualifying clinical pathways specifications with respect to privacy requirements. We believe clinical process modelling languages should be more adapted to a multidisciplinary clinical systems users' profile. Thus, we are planning to investigate the adoption of a variety of symbols and modelling patterns that are better tailored to the requirements of the clinical community.

REFERENCES

[1] U.S. Department of Health & Human Services HHS: HIPAA Privacy Rule Summary. [Retrieved: July, 2013].

http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[2] E. Rolón et al., “Process modeling of the health sector using BPMN: A case study” The First International Conference on Health Informatics-Diagnostic Pathology (HEALTHINF 2008) IARIA, Jan. 2008, pp. 173-178, ISBN: 978-989-8111-16-6

[3] S. Ferrante, S. Bonacina, G. Pozzi, F. Pinciroli, and S. Marceglia, “A design methodology for medical processes,” Applied Clinical Informatics, vol. 7, pp. 191-210, 2016, doi:10.4338/ACI-2015-08-RA-0111.

[4] F. Ruiz et al., “Business process modeling in healthcare,” Stud Health Technol Inform, vol. 179, pp. 75-87, 2012.

[5] R. Braun, H. Schlieter, M Burwitz and W. Esswein, “Extending a Business Process Modeling Language for Domain-Specific Adaptation in Healthcare” The 12th International Conference on Wirtschaftsinformatik in Osnabrück-Smart Enterprise Engineering (WI 2015), Mar. 2015, pp. 468-481, ISSN: 0937-6429, ISBN: 978-3-00-049184-9

[6] S. Bielack, D. Carrle, P. G. Casali, and ESMO Guidelines Working Group, “Osteosarcoma: ESMO clinical recommendations for diagnosis, treatment and follow-up,” Annals of Oncology, vol. 20, pp. iv137-iv139, May. 2009, doi: 10.1093/annonc/mdp154.

[7] V. Augusto, and X. Xie, “A modeling and simulation framework for health care systems,” IEEE Transactions on Systems, Man, and Cybernetics Systems, vol. 44, pp. 30–46, 2014.

[8] E. Rojas, J. Munoz-Gama, M. Sepúlveda, and D. Capurro “Process mining in healthcare: A literature review, ”Journal of biomedical informatics, vol. 61, 224-236, June 2016, doi: https://doi.org/10.1016/j.jbi.2016.04.007.

[9] N. Hashemian, and S. S. R. Abidi, “Modeling clinical workflows using business process modeling notation. In Computer-Based Medical Systems,” IEEE Computer-Based Medical Systems, pp. 1–4, June 2012 [CBMS 25th International Symposium Italy, 2012].

[10] R. Siegel et al., “Cancer treatment and survivorship statistic,” CA: a cancer journal for clinicians, vol. 62, pp. 220-241, Jul-Aug. 2012, doi: 10.3322/caac.21149.

[11] M. S. Isakoff., S. S. Bielack, P. Meltzer, and R. Gorlick, “Osteosarcoma: current treatment and a collaborative pathway to success,” Journal of clinical oncology, vol. 33, pp. 3029-3035, Sep. 2015, doi: 10.1200/JCO.2014.59.4895.

[12] A. Luetke, P. A. Meyers, I. Lewis, and H. Juergens, “Osteosarcoma treatment–where do we stand? A state of the art review,” Cancer treatment reviews, vol. 40, pp. 523-532, May. 2014, doi: https://doi.org/10.1016/j.ctrv.2013.11.006.

[13] A. Paioli, M. Rocca, L. Cevolani, E. Rimondi, Daniel Vanel, Emanuela Palmerini, Marilena Cesari, A. Longhi, A. M. Eraldo, E. Marchesi, P. Picci and S. Ferrari, “Osteosarcoma follow-up: chest X-ray or computed tomography?,” Clinical sarcoma research, vol. 7, Feb. 2017, doi: 10.1186/s13569-017-0067-5.

[14] M. C. Oetzel, and S. Spiekermann, “A systematic methodology for privacy impact assessments: a design science approach,” Eur. J. Inf. Syst., vol. 23, pp. 126–150, March. 2014, doi: https://doi.org/10.1057/ejis.2013.18.

[15] S. Rajamani, E. S. Chen, Y. Wang, and G. B. Melton, “Extending the HL7/LOINC Document Ontology Settings of Care,” AMIA Annual Symposium Proceedings, Nov. 2001, pp. 994-1001, doi: https://doi.org/10.1016/j.cmpb.2015.09.020.

[16] HIPAA Privacy Rule: Uses and disclosures of protected health information: General rules (§164.502). [Retrieved: January, 2013]. https://www.law.cornell.edu/cfr/text/45/164.502.

[17] HIPAA Privacy Rule: Uses and disclosures for which an authorization is required (§164.508). [Retrieved: January, 2013]. https://www.law.cornell.edu/cfr/text/45/164.508.

[18] Regulation (eu) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). [Retrieved: March, 2017]. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC.