Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 164 (2019) 706–713

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

Enhanced privacy governance in Health Information Systems through business process modelling and HL7

Hanene BOUSSI RAHMOUNI [a,b] ,Intidhar Essefi [b*], Mohammed Fethi Ladeb [c]

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

Abstract

Medical data privacy is nowadays an alarming issue thanks to the technological revolution witnessed in the medical field and the ease of data access and exchange leveraged by newly implemented Hospital Information Systems (HIS). In order to help protect patient data while offering them the required medical procedures, many computerized techniques could be made available to be implemented in HIS since an early stage of their design. Those techniques should be applied throughout the rolling of clinical pathways to preserve medical data privacy and security in order to enhance privacy governance within Hospitals. When considered as processes, and because of their complexity and multidisciplinary nature, clinical pathways should be modelled in a simple way paying attention to medical tasks and the underlining shared clinical data. It is important to highlight the data with higher protection and sensitivity level. These data characteristics will influence many governance and security decisions of each process. This work aims to present a methodology to model clinical pathway specifications for data driven clinical processes, distinguishing sensitive data from other data and identifying personal data protection principles and the Protected Health Information (PHI). In this context, we precise for each clinical task potentially involving data processing and sharing, the level of protection the data requires through the use of privacy tags and labels added to data elements predefined using the HL7 standard. This method of tagging would help mapping extracted data, classified into categories, to a set of privacy requirements as needed by the HIPAA legislation. Hence data protection and privacy governance are leveraged in a seamless and highly transparent way. The use of HL7 allowed better data discovery and parsing which facilitates the definition of medical data protection measures at a later stage.

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

10.1016/j.procs.2019.12.239

Keywords:
Business process, clinical care pathway, data protection, electronic exchanges, HL7, HIPAA legislation, patient privacy, privacy governance, privacy requirements, threats ;

1. Introduction

Information technology is nowadays widely implemented in the medical field in order to ensure electronic medical data exchanges and communication. Processing and treating medical data increase threats of personal data disclosure and illegal use. This is why; medical data management should comply with personal data protection laws; legislation and personal information management standards to ensure their safety while respecting and preserving the patient's privacy. Personal medical data are mostly processed throughout clinical pathways enforced by Hospital Information systems. They are shared and communicated between healthcare professionals to ensure care continuity and to enhance care quality; sometimes; via secondary use of medical data. Indeed, the necessity of electronic medical data processing and management particularly for secondary use purposes such as public health and research increases the risks related to its use and disclosure.

Personal medical data are widely used by all routine and advanced clinical processes. They are useful for medical workflows and processes rolling. They are electronically exchanged, manipulated and processed between healthcare providers either for direct care or secondary use purposes. For those reasons, high risks of disclosure and illegal use of personal data are always present with relation to personal data, medical tasks and processes. Furthermore, security measures ought to be defined according to sensitive data types and its underlined privacy risk level in order to enhance patient privacy governance within the hospitals' boundaries and beyond them. However, in order for these privacy risks to be evaluated and specified, it is essential to first capture and analyze the existing clinical workflows and medical processes responsible for handling and processing the protected data/documents. A first step towards this goal should be a clear representation of these automated processes using a standard process modelling language such as BPMN (Business Process Model and Notation) [1].

In this paper, we propose a methodology to enhance privacy governance in HIS throughout clinical business process modelling and HL7 standard [9]. Our approach is based on highlighting shared clinical documents throughout modelling clinical processes. Then, based on HL7-CDA standard [11], we extracted and identified sensitive data within the shared clinical documents. After that, we identified data protection principles and highlighted applicable PHI according to the HIPAA legislation [15]. Afterwards, we mapped each sensitive data category to the required computerized security method in privacy compliance with HIPAA Privacy Rule which ought to be implemented in HIS development to enforce personal data protection. In this work, osteosarcoma was used as a case study to validate our approach.

This paper is divided as follows: in Section 2, we present the osteosarcoma clinical pathway processes subject to study as well as the clinical pathway modelling language of our choice. We adopt a data-oriented clinical pathway modelling approach. In Section 3, we present our shared clinical data and document architecture retrieved from the studied clinical processes and matched with HL7 data and document model. In Section 4, we define personal data protection law principles and Privacy requirements for PHI. Then we identify the set of security labels to be implemented for clinical data protection during process execution. Finally, in Section 5, we present the conclusion and future work.

2. Clinical care pathway processes modelling : Osteosarcoma case study

Oncological pathologies' care pathways are well-known by their difficult management facts with complex and multidisciplinary procedures and processes. They usually require the participation of healthcare providers from different medical departments and specialties. These pathways are based on three main phases which are the diagnosis,

the treatment and the follow-up procedures. In this work we chose the osteosarcoma as a case study. The osteosarcoma is an oncological pathology. It is known as a fetal bone cancer. Besides, it is a primary malignant bone tumor. The average of people who are estimated to be diagnosed with osteosarcoma in the United States vary between 800 and 900 each year. It affects those aged between 10 and 30. Under the microscope, osteosarcomas can be classified according to the cells' behavior as high, intermediate or low grade [2].

According to the NCCN (National Comprehensive Cancer Network) and the ESMO (European Society for Medical Oncology), the osteosarcoma care pathway includes very complex clinical processes. It begins from the diagnosis, going through the treatment and ending with the follow-up. Affected person usually does not feel sick. However, they may have a history of pain in the affected area or develop a limp. The felt pain does not go away with rest, it is related to muscle soreness or growing pain. As a consequence, the osteosarcoma is discovered further to an injury or a pathological fracture (the tumor weakens a bone, so it breaks). The first diagnostic test that patients receive is an x-ray after visiting the doctor. If it is recognized that a bone cancer is diagnosed then several additional tests are critical for the cancer diagnosis and staging. An entire bone MRI should be performed to locate the primary tumor with ruling out metastases. A chest x-ray and CT-scan are performed to detect lung metastases. In addition a body bone scan (scintigraphy) is performed to rule out distant spread of the tumor. To define the tumor characteristics, a biopsy provides a definite diagnosis. Imaging studies and biopsy results allow doctors to stage the cancer and decide about the treatment plan. It consists in performing some tests focusing on the heart, kidneys, liver and hearing in order to monitor the patient health during treatment. It is principally based on chemotherapy, surgery and radiotherapy depending on the patient's response to the therapy. Once the treatment phase is fulfilled, it is recommended to schedule follow up exams and tests. Generally, most appointments include physical exam, original cancer's location imaging and chest imaging. As for the tests, they are periodically done to monitor the heart, the liver, the kidneys, the hearing loss as well as checking hormone levels, bone density and cholesterol [3][4].

Guidelines on healthcare information processing, communication and sharing between the involved medical professionals among medical services within clinical care pathways should be enforced by implemented HISs in healthcare facilities. Each clinical pathway includes a set of processes containing on its turn sets of tasks. They are carried out throughout the three care pathway typical phases in order to communicate medical documents and clinical data as required by the specified care pathway [5].

When sensitive clinical data are communicated between healthcare providers, their identification is required for the purpose of providing a transparent care pathway standard specification. Besides, their protection is required by personal data protection law. Therefore, we modelled the osteosarcoma clinical pathway in the form of clinical business process models. In the following subsection, we present the modelled data driven clinical care pathways of only the diagnosis phase of the osteosarcoma clinical pathway using the BPMN standard. Other phases of the process will be represented in future work.

2.1. Osteosarcoma diagnosis clinical care pathway

Fig. 1 presents the diagnosis phase of the osteosarcoma clinical pathway model. It gives attention to the communicated clinical documents throughout the care pathways of the diagnosis phase. Besides, it presents the process's steps required by the diagnosis clinical care pathway of the osteosarcoma. According to the physical examination and the symptoms findings, some medical tests as medical imaging tests are performed to accomplish the check-up phase and identify the pathology. If the imaging findings present any osteosarcoma doubt then a CT Scan examination is needed to exclude malignancy. In case cancer malignancy is not excluded then anatomopathology test and entire bone MRI are performed in order to confirm the tumor malignancy. Moreover, Bone scintigraphy and Thoracic XRay are performed to evaluate metastasis and stage the tumor. The treatment plan and procedure is defined according to the all previous findings. As a consequence, the osteosarcoma clinical pathway of the diagnosis phase is complex and involves collaboration of healthcare providers and diverse medical services. It is based on the communication and the share of several medical documents types (e.g., reports, orders, images, etc.) and subtypes (e.g., imaging report, anatomic pathology report, etc.) between healthcare providers within the patient's Shared Medical Record (SMR)[6].

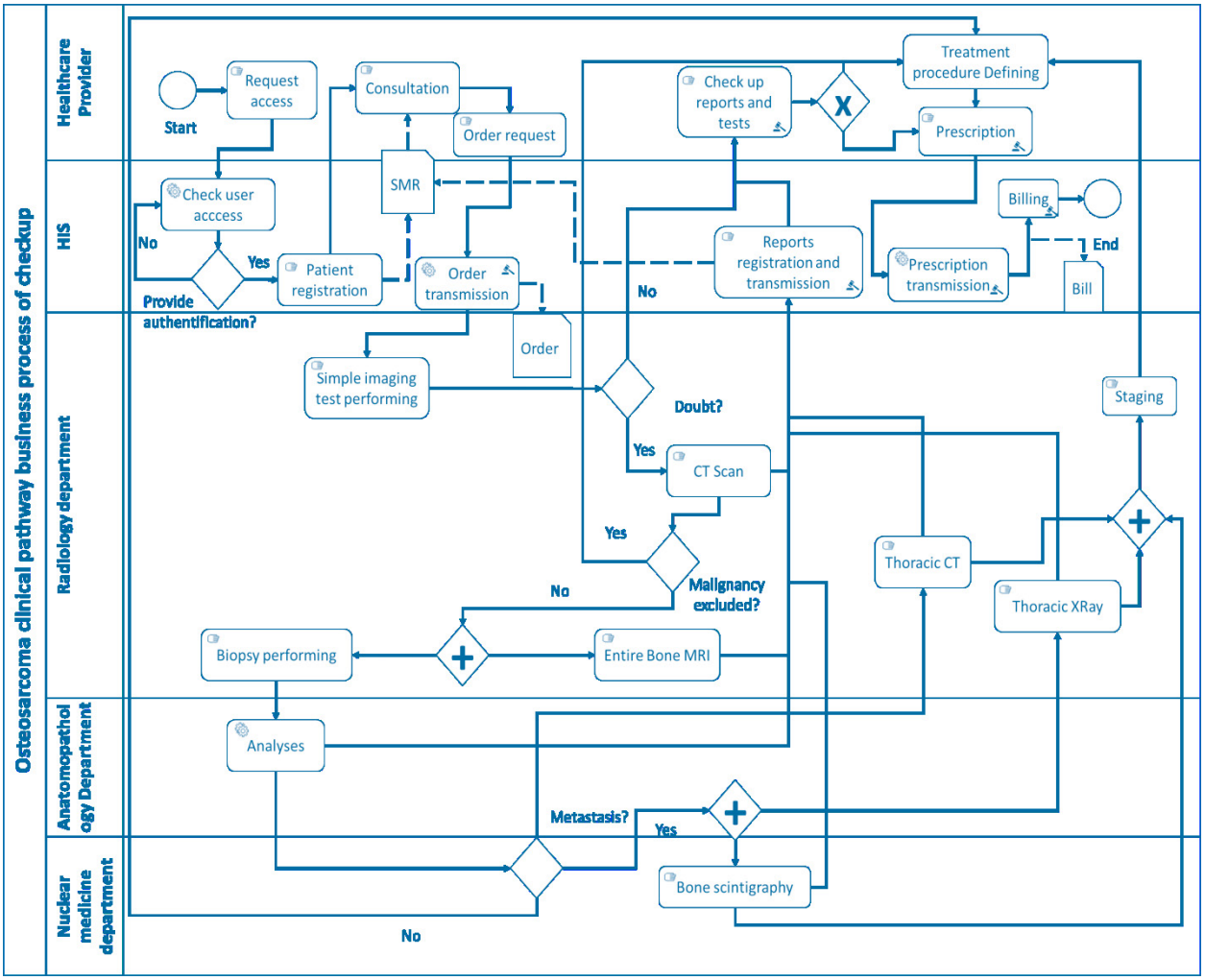

Fig. 1. Osteosarcoma diagnosis clinical pathway business process

3. Exchanged clinical document architecture

Patient Electronic Health Record presents a main of patient medical data communication between healthcare professionals. It includes all medical data types and medical documents categories. In general, the most used medical documents are therapeutic data, nursing notes, problem lists, detailed orders, diagnostic test data, socio-economic data and procedure data. Therefore, we could classify medical documents into a set of categories and subcategories. Shared and communicated medical document within SHR include all types of clinical documents as medical history record, discharge summary, typical paper chart, mental status examination and medical reports like medical tests and operative reports. Various clinical data types are used. They could be found in the form of narrative text recorded by clinician, numerical measurements (eg. blood pressure, temperature, lab results, etc.), textual data (results reported as a text), recorded signals (eg. EKG, EEG, etc.) and pictures (eg. Radiographs, photographs and other images). All the previous data are useful for many purposes. They may be used to be the basis of historical record, to support communication among providers, to anticipate future health problems, to record standard preventive measures. Besides, they could be required for coding and billing, providing legal record or supporting clinical researches.

Medical data are not only used for patient healthcare but for some secondary uses either. Moreover, medical data secondary uses' purposes are revolving around identifying target patient cohort(s) for clinical trials, observational

studies of drug benefits and adverse effects, clinical quality improvement for patients (e.g., for diabetes), monitoring errors (e.g., in the emergency room), analyzing rates of use of medication to prevent certain conditions (e.g., blood clots) and monitoring the type of lab test requests [7]. Each clinical document is composed of many fragments. It provides information about patients, procedures, physicians and assistants, diagnoses, findings and appointments within clinical document fragments as shown in [6]. Each data type has a set of specifications to respect. The sensitive one should be protected and privacy compliant manner throughout the implementation of privacy requirements since an early stage of HIS development. This should be applied to the PHI as required by the HIPAA Privacy Rule [7][8].

Based on the HL7-CDA standard, we could map the shared medical documents to a set of characteristics aiming to facilitate the representation of the processed medical data throughout the modelled care pathway of the osteosarcoma. Each clinical document includes a set of attributes. They provide information about the document name, category (e.g., medical reports, medical record, etc.) and its architecture. The included content of the medical documents could be classified into a set of metadata, data and values.

According the CDA standard [9], a clinical document is divided into two main parts. The first part is known as the document's header. It provides information about the document name, type and version. It also affords information about participants, organization, etc. As to the second part, it is known as the clinical document's body. It affords information about the body content. So, it details information as the findings, the reason for study, the history, procedure context, the study act and the observation. Therefore, we could map the clinical documents content to the described structure in [10]

Each clinical document includes data structured in a hierarchical way that specifies the recommended content in the form of sections (eg., participants, authorization, clinical statements, etc.). For example for the participants section in the header of the imaging report [11], we found record target representing the patient's information, author, data enterer, information recipient, legal authenticator and participant as sub sections. For each sub section, a set of data values are required to be assigned while the document is processed and managed within the patient care pathway building the medical processes of the hospital information system. As illustrated in [12], the record target (patient) sub section affords information about the patient role which includes address, phone number, patient name, birthdate and gender.

4. Privacy requirements for protecting sensitive data

Medical data use and management ought to be compliant with international law frameworks of personal data protection. Those law frameworks are based on the described data protection principles in [13][14]. Healthcare data management presents risks threatening a person's life and may affect both his privacy as well as his professional life. For that, they are governed by many jurisdictions, namely, HIPAA Privacy Rule [15] and the GDPR framework [16].

Medical data are used for many purposes. They may be used for the patient healthcare as asking for a second opinion, or for research etc. in order to enhance the quality of care. This increased interest in medical information has also increased the potential for unauthorized usage and disclosures of personal health information. For each purpose of use, there is the involvement of some required and optional data. Therefore, we need the implementation of a security adaptable model within HIS to match the required data to its level of sensitivity and security process. Access control system implementation is required to protect medical data against any unauthorized process. The adoption of data centric care pathways modelling during the development process helps to highlight the medical documents to be processed within each process or workflow. It also allows us to detail and classify data within the clinical documents into categories indicating its level of sensitivity and demand for protection. The HIPAA Privacy Rule defines a set of information called Protected Health Information (PHI) as detailed in [17].

This information is considered as individual identifiable information. In addition, HIPAA Privacy Rule has defined a set of rules to preserve the patient rights with respect to medical information use and disclosure. According to the medical data disclosure purposes, the Privacy Rule defined the access control requirements, the permitted uses and disclosures with and without patient consent or authorization and when it is permitted to break the glass [8][18][19].

An adaptable security system development to the security requirements is required to help HIS developers to pay attention to patient security measures from an early stage of the HIS's design. This could be used to enforce the principle of "minimum necessary" information use [15]. For that, attaching security labels, as the described examples

in Table 1, to the medical data is necessary to control human and system behavior while processing sensitive medical data.

Labeling data with security attributes or tags could provide an important mechanism to enhance data protection [20]. These labels are widely used for controlling data access according to its sensitivity, which is based on an analysis of applicable privacy policies while taking into consideration some related ethical and socioeconomic issues to the individual and to the organization controlling the hosted data. Therefore, security labels implementation ensures the correlate user and medical document access. This presents a mean defense against data disclosure and unauthorized use. When medical data are electronically communicated, it is desirable to enforce security policy throughout the processed care pathway. This ensures that the information is not sent to someone that does not have an appropriate authorization. This is why we are providing this security model, as illustrated in Table 1, which will be enhanced in a future work. Examples of these security labels should include tags related to many properties of the data as described in [21]: Usage restriction (i.e. highly restricted, restricted, restricted with exemption and partially restricted use of sensitive data that identify the subject). Actual protection status (i.e. in clear, anonymization, encryption, obfuscated, watermarked and hidden, has proof of integrity…)[22][23][24][25] and many others.

Table 1. Examples of security tags for sensitive data.

	Security tags	Examples	Description
Usage restrictions	Loose/non-personal	publicly available information: business name, phone, email or physical address	Indicating that the information is not classified as sensitive.
	Ordinary	logistics, payment, or operations	The information is typical and presents typical risk of harm if disclosed without authorization.
	Highly Restricted	Information about a victimisation of abuse, patient requested information sensitivity, etc.	Indicates that the information is extremely sensitive. It presents a very high risk if disclosed without authorization
	Restricted to a group of experts	Sensitive conditions mental health, HIV, substance abuse, genetic disease, and reproductive health.	Indicating a high sensitivity of data. It presents a high risk to the information subject if disclosed without authorization.
	Restricted with Exemption	A researcher conducts: studying treatment outcomes for a certain drug.	Research with human subjects may qualify for an exemption. The information is recorded in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects.
	Partially Restricted	Accessed by a wider range of personnel not all of whom are actively caring for the patient such as radiology staff	Only some fields of the document should be restricted
Actual Protection Status	In clear	Care, treatment, payment	Requires minimal data protection security in order to allow authorised medical users to have fast and seamless access to data (or example during emergency care). Or other administrative data that doesn't require protection.
	Anonymized	Transfer of information across a boundary	Process of removing personally identifiable information from data sets
	Encrypted	Exchanging medical data using email programs	Transform data into a form in which there is a low probability of assigning meaning
	Obfuscated	preserves privacy of the shared data (cluster analysis)	Embedding identification codes into host media
	Watermarked	Inserting meta-data to render the image more usable and information protection with application like integrity control	The insertion of a message within the image, also called content or watermark message, in a host document in some multimedia format
	Hidden	Users could have only partial access to patient data. For example, a receptionist could not see results of medical tests	Using SQL queries or database views to filter the data before allowing access
Legal compliance and safeguards		Securing medical records with locks and keys or pass codes	Covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information

Consent necessity	Individual informed consent	Ask a patient to consent to receiving therapy before providing it	Getting permission before conducting a healthcare intervention on a person, or for disclosing personal information.
	Group consent	Population genetics research on groups	Used for collecting, processing, use and transferral of indigenous samples and data.
	General consent	Receiving diagnostic tests	Authorizing the practitioner to render care
	Specific consent	Abortions, sterilization	Used in a specific purpose or healthcare procedure.
Intellectual property rights		Scientific reports discussing a new discovery or innovative approach involving patient data.	Any systematic investigation designed to develop or contribute to generalizable knowledge.

5. Conclusion and future work

Data-centric business process modelling applied to care pathway was a necessary step for highlighting shared clinical data. Nowadays, the medical field has experienced a revolution with regard to hospital information systems and medical procedures processing and management. Therefore, several business process modelling languages such as IDEF 0, IDEF 3, UML 2.0 and BPMN, are made available to model and represent clinical pathways [1]. Making these process notations more data aware allows clinical care pathways to be more efficient and reliable in preserving patient privacy. Within the BMPN care pathway models, we highlighted clinical data used in each process. These data elements were associated with their equivalent data elements and documents as defined by HL7-CDA document architecture. A detailed description of this phase of the work will be however described in a more extended version of the paper. Combining process and data discovery techniques has allowed for a deeper understanding and analysis of existing pathologies and the performed activities on the working floor to discover care pathway inefficiencies. Modelling care pathways in the form of clinical processes allowed to overcome their complexity and to define their requirements regarding patients' privacy and health care professionals [26][27]. Still, privacy and security challenges are increasing while managing medical data with respect to the required technologies implementation [28].

In our work we have tackled this issue by defining some general rules of HIPAA privacy requirements with relation to patients identifying medical documents, their use and disclosure, since personal data processing must obey to privacy protection laws. 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 puts the emphasis on an orthogonal integration of privacy obligations throughout the clinical process using security labels. In this context, we propose in a future work to develop an adaptable clinical process model dealing with both the human and the system aspects of privacy management when processing protected health data. This will ensure an explicit privacy specification based on clinical data highlighting and labelling as part of clinical processes design and implementation.

References

[1] RUIZ, Francisco, GARCIA, Felix, CALAHORRA, Luis, et al. Business process modeling in healthcare. Stud Health Technol Inform, 2012, vol. 179, p. 75-87.

[2]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.

[3] Casali, P. G., Bielack, S., Abecassis, N., Aro, H. T., Bauer, S., Biagini, R., ... & Brodowicz, T. (2018). Bone sarcomas: ESMO–PaedCan–EURACAN Clinical Practice Guidelines for diagnosis, treatment and follow-up. Annals of Oncology, 29(Supplement_4), iv79-iv95.

[4] Biermann, J. S., Chow, W., Reed, D. R., Lucas, D., Adkins, D. R., Agulnik, M., ... & Didwania, A. (2017). NCCN guidelines insights: bone cancer, version 2.2017. Journal of the National Comprehensive Cancer Network, 15(2), 155-167.

[5] REBUGE, Álvaro et FERREIRA, Diogo R. Business process analysis in healthcare environments: A methodology based on process mining. Information systems, 2012, vol. 37, no 2, p. 99-116.

[6] Essefi, I., Boussi Rahmouni, H. and Ladeb M. F., Data Driven Medical Process Modelling for Privacy Protection in Care Pathways, The Seventh International Conference on Global Health Challenges, 2018, p. 24-31.

[7] WANG, Yan, PAKHOMOV, Serguei, DALE, Justin L., et al. Application of HL7/LOINC document ontology to a university-affiliated integrated health system research clinical data repository. AMIA Summits on Translational Science Proceedings, 2014, vol. 2014, p. 230.

[8] WRIGHT, David. The state of the art in privacy impact assessment. Computer Law & Security Review, 2012, vol. 28, no 1, p. 54-61.

[9] HL7 standard. Available from: http://www.hl7.org/implement/standards/index.cfm?ref=nav

[10] Smits, M., Kramer, E., Harthoorn, M., & Cornet, R. (2015). A comparison of two Detailed Clinical Model representations: FHIR and CDA. European Journal for Biomedical Informatics, 11(2).

[11] Mense, A., & Blobel, B. (2017). HL7 standards and components to support implementation of the European general data protection regulation. European Journal for Biomedical Informatics, 13(1), 27-33.
[12] Takeda, T., Ueda, K., Nakagawa, A., Manabe, S., Okada, K., Mihara, N., & Matsumura, Y. (2017). A Document-Based EHR System That Controls the Disclosure of Clinical Documents Using an Access Control List File Based on the HL7 CDA Header. Studies in health technology and informatics, 245, 1238-1238.
[13] Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134-153.
[14] Ahluwalia, S., & Bandyopadhyay, T. K. (2018). Data protection in medical research: A comparative analysis. Journal of Data Protection & Privacy, 1(4), 345-355.
[15] HIPAA Privacy Rule. [Online]. Available from: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/privacyrule/privrulepd.pdf
[16] MENSE, Alexander et BLOBEL, Bernd. Hl7 standards and components to support implementation of the European general data protection regulation. European Journal for Biomedical Informatics, 2017, vol. 13, no 1, p. 27-33.
[17] DROLET, Brian C., MARWAHA, Jayson S., HYATT, Brad, et al. Electronic communication of protected health information: privacy, security, and HIPAA compliance. The Journal of hand surgery, 2017, vol. 42, no 6, p. 411-416.
[18] HIPAA Privacy Rule: Uses and disclosures of protected health information: General rules (§164.502). [Online]. Available from: https://www.law.cornell.edu/cfr/text/45/164.502, last reviewed: 2013.
[19] HIPAA Privacy Rule: Uses and disclosures for which an authorization is required (§164.508). [Online]. Available from: https://www.law.cornell.edu/cfr/text/45/164.508, last reviewed: 2013.
[20] ZHENG, Lantian et MYERS, Andrew C. Dynamic security labels and noninterference. In : IFIP World Computer Congress, TC 1. Springer, Boston, MA, 2004. p. 27-40.
[21] HL7-FHIR standard. [Online]. Available from: https://www.hl7.org/fhir/secpriv-module.html, last reviewed: 2018
[22] BAO, Shu-Di, CHEN, Meng, et YANG, Guang-Zhong. A method of signal scrambling to secure data storage for healthcare applications. IEEE Journal of Biomedical and Health informatics, 2017, vol. 21, no 6, p. 1487-1494
[23] HOLLA, Seema et DALA-KRISHNA, Praveen. Medical data encryption for communication over a vulnerable system. U.S. Patent No 7,974,924, 5 juill. 2011.
[24] AZARIA, Asaph, EKBLAW, Ariel, VIEIRA, Thiago, et al. Medrec: Using blockchain for medical data access and permission management. In : 2016 2nd International Conference on Open and Big Data (OBD). IEEE, 2016. p. 25-30.
[25] COATRIEUX, Gouenou, LECORNU, Laurent, SANKUR, Bulent, et al. A review of image watermarking applications in healthcare. In : 2006 International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE, 2006. p. 4691-4694.
[26] CHRISTOV, Stefan, CHEN, Bin, AVRUNIN, George S., et al.Formally defining medical processes. Methods of Information in Medicine, 2008, vol. 47, no 05, p. 392-398.
[27] REBUGE, Álvaro et FERREIRA, Diogo R. Business process analysis in healthcare environments: A methodology based on process mining. Information systems, 2012, vol. 37, no 2, p. 99-116.
[28] Kotz, D., Gunter, C. A., Kumar, S., & Weiner, J. P. (2016). Privacy and security in mobile health: a research agenda. Computer, 49(6), 22-30.