An interdisciplinary approach for security, privacy and trust in the electronic medical record

A pragmatic legal perspective

Léonore Cellier
Swiss Cybersecurity Advisory Group (SCARG)
University of Lausanne (Faculty of Law)
Switzerland
leonore.cellier@unil.ch

Solange Ghernaouti
Swiss Cybersecurity Advisory Group (SCARG)
University of Lausanne (HEC)
Switzerland
sgh@unil.ch

***Abstract*—The use of electronic medical records in healthcare institutions is becoming more widespread, bringing benefits in terms of quality, security and efficiency of patient care. The development of e-health, i.e. the integrated use of information and communication technologies and services, is considered a performance factor in medicine. The purpose of this article is to identify the key success factors of cybersecurity for e-health and to demonstrate that the effectiveness of cybersecurity depends on the complementarity of organizational, managerial, human, legal and technical measures. Technical innovation alone cannot meet the requirements of security and trust. The latter must be achieved through organizational policies that take into account the needs of each party. Our research was conducted from a European perspective and focused on Swiss university hospitals and the laws applicable to them. Since the issues are similar everywhere, however, the recommendations are generic, global and effective in different countries.**

Keywords - medical data protection; electronic medical record security; GDPR; trust; privacy; technico- legal complementarity; cybersecurity culture.

I. INTRODUCTION

In hospitals, patient data face two contradictory needs. On the one hand, they must be quickly accessible to many individuals at all times in order to ensure efficient care, but they also require protection because they affect the person's privacy. According to article 15, paragraph 2 of the General Data Protection Regulation (GDPR) [1], this information essential to care, consists, of data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

These elements are mainly transmitted via an information system that manages electronic medical records. An Electronic Medical Record (EMR) is a computerized medical record created in an organization that delivers care, such as a hospital or physician's office, for patients of that organization. Ideally, EMRs should be shared between providers and settings to provide a detailed history of contact with the health care system for individual patients from multiple organizations [2]. In Swiss hospitals, these files are open to medical, administrative and technical staff without restriction in order to meet the need for rapid care. Unfortunately, in many cases, it appears that information is seen or processed for purposes other than the continuation of hospital services.

A question therefore arises concerning the management of these systems: do we want to control the handling of the medical file or can we trust staff fully to respect privacy.

Neither option is possible since both interests are of similar importance. The solution therefore lies in leaving the data accessible but by setting up monitoring. How then can we guarantee and check that the information is only used for care purposes? How can we find a system whereby effective security does not hinder the use of software by medical staff?

After an analysis of the current system, in particular, through observations of current hospital practices, surveys of IT security managers and lawyers from Swiss university hospitals, doctors and patients (Section II), we propose a set of complementary pragmatic recommendations that provide security of information through a balance of interest between the need for control, ease of use and trust in medical record systems (Section III).

II. ANALYSIS OF THE CURRENT SYSTEM

It is customary for each doctor to keep a medical file, which includes all documents concerning the patient, in particular the anamnesis, the result of the clinical examination and analyses and the assessment of the patient's situation, the proposed and actual care provided, with an indication of the author's name and the date of each registration. In Switzerland, the file may be in paper or digital form provided that any addition, deletion or other modification remains detectable and that its author and date can be identified.

A. Electronic medical records are widely accessible

In view of the increasing number of staff members having to treat the same person, access to medical files must be open to the professionals concerned. As far as electronic medical records in clinics, practices or hospitals are concerned, it is surprising to note that physicians have wide access to all records, for the simple reason that this facilitates patient management. At the Hôpitaux Universitaires de Genève (HUG), for example, any member of the medical staff can open and modify the patient's file.

978-1-7281-0402-7/19/$31.00 ©2019 IEEE

Although some information is useful for all the specialties of a health care facility, not all of it should be shared [3]. Some is very specific and should only be accessible to a specialist. However, the structuring of primary systems and the classification of data in terms of usefulness to the various services are so complicated that access to all medical personnel is preferred.

The data protection officer of the Canton of Berne states in this respect that the patient's consent is presumed but, if he wishes, he can specify to the hospital whether or not the information should not be transmitted to other healthcare providers. However, the patient should be warned that such a restriction may affect treatment, for example if the family doctor does not have the necessary information [4].

This seems surprising because it contravenes certain data protection principles. For example, the second paragraph of section 4 of the Swiss Federal Act on Data Protection (FADP) [5] states that the processing must comply with the principle of proportionality, i.e. it must be necessary for the purpose intended. Article 5 (1) (c) of the GDPR requires that data be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization')*". In other words, a measure must not go beyond what is reasonable. In this sense too, the processing operation may not be carried out beyond a specified and appropriate time. In short, no data can be processed with specific limits [6].

Under this principle, only those who have to care for a patient are supposed to know their pathologies and therefore have access to the medical records. Yet in a hospital, because of the need to communicate the information as quickly as possible in an emergency and to facilitate care, a neurosurgeon can access gynecological information about people who are not her/his own.

The data must also be processed for defined purposes (Article 5 (1) (b) GDPR), i.e. only for the purpose stated at the time of collection, which is provided for by law or which arises from the circumstances. When other professionals access the file, it is therefore necessary to check whether the purpose of the collection authorizes these third parties to receive the information [7]. Indeed, even if medical data are, to a large extent, transmitted by patients themselves to health care institutions, and their consent is often implicit for the information to be transmitted. There is no certainty that the data are processed just for their specific goal.

For example, it has been reported that a secretary in charge of human resources at a university hospital had access to an employee's medical file. She was able to reveal details of a very intimate operation. In this case, it appears the processing was lawful at the time of collection since it was necessary for the patient's treatment, but it became unlawful at the time of communication since the information should not have been submitted to the secretary.

To ensure that employees comply with these data protection principles, the various hospital structures studied have implemented access control measures (*B*).

B. Control through logs and social control

The efficiency of care is ensured through digitized patient records since they are accessible to a large number of professionals in many locations. This broad communication of data must nevertheless be controlled in order to limit abuse, particularly within large institutions. A high risk of intrusion exists since all staff have the opportunity to access data. Relying on the goodwill of staff seems to be a solution when steps are taken to raise awareness of the legal and ethical aspects of medical confidentiality [8]. However, the patient is never immune to the risk of invasion of privacy. Logging control of all access to a file therefore seems to be a valid solution to ensure the confidentiality of information.

In Switzerland, the logging procedure is provided for in Article 10 of the Ordinance on the Data Protection Act. It must be implemented by the controller of the file if preventive measures are not sufficient to guarantee data protection. It is also necessary when, without it, it would not be possible to verify retrospectively that the data have been processed in accordance with the purposes for which they were collected or communicated. Logging records are kept for one year. They are accessible only to the persons responsible for verifying the application of the provisions on the protection of personal data and are used only for this purpose.

In addition to logging access, the HUG have implemented the "social control" system, requiring the 12,000 staff members who suspect undue access by another employee to report it. This system works because the logs appear in the medical record file. For a doctor in charge of a 24-year-old diabetes patient, it will be easy to see that a nurse in the Geriatrics had no reason to consult the file in question. The doctor can then report the nurse to the hospital legal department. However, while this system appears to be very effective, it is rarely used by the doctors because they are reluctant to report their colleagues and do not have much time to devote to such action during work. It is only used in serious cases.

Finally, this social control has other benefits: by seeing the names of the people who have accessed the file, the collaborator can contact his predecessor in order to be informed about the patient. There is thus a significant proven efficiency in terms of care and a probable efficiency in terms of access control, but which will take time to become established if employees are encouraged to follow the guidelines. Pending such practices, the law sanctions breaches of privacy (*C*).

C. *An existing legal framework but a lack of a culture of medical privacy and cybersecurity awareness*

In addition to technical measures for monitoring access, health professionals are subject to medical confidentiality. This has its origin in the Hippocratic Oath, which has become a custom and which obliges each practitioner to respect any information entrusted to him. Secrecy concerns everything a patient reveals to his doctor but also all the information the latter discovers during the medical examination. It refers to medical data but also to personal data concerning the family, profession or financial situation of the patient [9]. While it is one of the oldest data protection principles, it is nowadays considered to be the cornerstone of the doctor/patient relationship, in the absence of which treatment is unthinkable because it guarantees trust between patient and doctor on the one hand and protects the private sphere as an individual interest on the other hand [10].

While its violation is severely sanctioned by different laws, not all persons are deterred to the same degree. Articles 320 and 321 of the Swiss Criminal Code (CC) [11] punish officials and doctors, dentists, chiropractors, pharmacists, midwives, psychologists and their assistants, who have revealed a secret entrusted to them by virtue of their profession or of which they became aware in the exercise of it. The violation occurs when the person intentionally makes the secret accessible to an unauthorized third party [12]. The penalty may be up to three years' imprisonment. However, while all staff of public institutions and health professionals are strictly controlled by these laws, it should be noted that stretcher-bearers, nursing assistants, secretaries or cleaning staff employed in private institutions are not.

In addition to these criminal articles, the Federal Act on Data Protection also imposes a professional confidentiality in Article 35. The penalty for this contravention is only pecuniary and is therefore less severe than that applied to Criminal Code offences. Nevertheless, the obligation of discretion has a much wider personal scope [13]. It is aimed at persons who unlawfully disclose secret and sensitive data known in the exercise of a profession but also in the context of an activity carried out on behalf of the person subject to professional secrecy. This less severe sanction applies only to persons not subject to the secrecy of articles 320 and 321 of the Criminal Code, thus filling a gap due to limited personal fields of application.

Civil servants and cares covered by the Criminal Code are no longer the only employees supervised by this law. A beautician who is informed of her clients' personal health background for the purpose of the care she provides, is also subject to the professional confidentiality, as is a data scientist, who, commissioned by a pharmaceutical group, will observe sensitive customer data.

Section 35 of the FADP is therefore applicable to all professionals with access to an electronic medical record. It is through these people, that much undue accessing of files takes place and leads to the disclosures of sensitive information. In the HUG, complaints are frequently sent to the legal department because people have breached the professional confidentiality. These are the main complaints that the service receives and is due to the fact that part of the staff is not at all aware of such a law and will respond positively to a request from third parties who wish to have information about a person who has consulted the hospital.

A delicate situation that can also arise with regard to technical maintenance. For example, IT managers are required to troubleshoot and repair bugs during the performance of their duties and therefore see sensitive information. According to some authors [14], they have the status of auxiliaries and are therefore subject to Article 321 CC. To acquire this status, the person must facilitate or support in one way or another the work of the professional and thereby become aware of confidential information, regardless of whether he or she is engaged on the basis of a contract, a mandate or acts as a simple volunteer. However, in other cases, the person must be under the direction or supervision of someone of the professions listed in Article 32 when performing the task. As this question is controversial, we believe it is appropriate to assume that, since computer scientists are not subject to professional or official secrecy if they are not civil servants or members of the governing body, they are only subject to the professional confidentiality.

If data are largely protected by various regulations, better monitoring and control of the application of these standards in systems must be put in place (Section III). It is regrettable that there is no concrete internal measure for monitoring access to EMR, since the system currently emphasizes communication rather than data security.

III. RECOMMENDATIONS PROPOSAL TO BUILD TRUST IN THE MEDICAL RECORD SYSTEM

Based on an analysis of the current environment, we can say that patients today cannot trust the privacy of their medical information since the evidence of medical secrecy is not demonstrated. To develop such reliability in computerized patient record, more control must be exerted. We propose several recommendations that seem fundamental to a high level of security in medical information system. This proposal is based on Swiss findings, but the idea could be transposed to many other countries since the issues are the same everywhere.

A. *A necessary compliance with the GDPR*

We assume that all information must remain accessible, particularly because of the emergencies and the potential inability of the patient to authorize access. Limiting access in hospitals is often difficult because patient treatment is dynamic. To provide exceptions to access control policies, previous work has evaluated if allowing employees to escalate their permissions would provide a reasonable compromise (these escalated accesses are specially logged

and reviewed). Unfortunately, employees escalated their permissions for over 50% of the patients [15].

It appears therefore that the management of access and data availability could be controlled differently to what the current system proposes. In our opinion, the HUG's social control does not prevent abuse related to the accessibility of files by all.

With the arrival of stricter regulations on data protection such as the GDPR, the requirement for security by default should be better taken into account by health care institutions. According to article 25, paragraph 2 of the GDPR, "*The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons*.". We can thus offer a scalable access system to ensure that it is put in place for the intended purpose in accordance with data protection principles. The system should limit access to the patient's carers. We must therefore find appropriate presetting, ensuring that only the personal data necessary for the purpose of the processing are handled by a limited number of users.

- **1st recommendation:** The file of a patient who is not under treatment should be unavailable. During this period, only administrative data allowing an individual to be identified must be accessible and readable.
- **2nd recommendation**: When the patient enters the hospital, the file must become available. The physician will search for the file on the database and then make a request for consultation and modification. This must be systematically authorized and should only be checked retrospectively.
- **3rd recommendation**: It will then be necessary to restrict access according to the services involved [16]. Indeed, the studies admit that it is necessary to limit access a priori, in a preventive way [17]. For example, a medical record open to the emergency services cannot be visible or available to employees in other areas. If the patient has to change services, the record should be transferred and the access rights of the first service deleted. An option in the system structure must be possible so that polymorbid patient records are accessible to several departments at the same time.
- **4th recommendation:** Within these services, access still needs to be divided up according to the roles and rights assigned to each:
  1. Caregivers (doctors, nurses, trainees) have access to everything.
  2. Administrative staff have access only to the data necessary for administrative processing, from making appointments to invoicing for insurance purposes. It appears that secretaries often see the whole file even though it is not part of their role. In our opinion, automatic coding processes could be developed to describe the pathology, care and drugs administered, etc.
  3. IT staff also have access to everything.

  To automate this process, recent work has examined predicting an employee's department or role using EMR audit logs. These roles have the potential to be used in a role-based access control system if highly accurate [15].
- **5th recommendation:** The file should be made unavailable once the consultation is completed. It is therefore necessary to determine when.

This EMR modeling appears to be both the most compliant with the security-by-default principle and the most viable in terms of accessibility and availability of information. However, these requirements must of course be supplemented by control measures (*B*).

B. Establish effective control through organizational measures

The arrangement of access as defined in the previous section makes it possible to limit abuse but does not result in a "zero risk". As the information remains permanently readable, it is necessary to establish a specific control to prevent abuse.

In Switzerland, public hospitals have a data protection officer who is responsible for ensuring compliance with the regulations in force. With the arrival of the GDPR in Europe, such a profession is becoming more widespread since each public establishment on EU territory is obliged to appoint a Data Protection Officer according to Article 37 of the Regulation. This officer is empowered by Article 39 to monitor compliance with the regulation. It could then be established that he controls the register of processing activities provided for by Article 30. Sanctions in the event of undue access could then be provided for and ordered by this officer.

A posteriori control seems indeed necessary since it allows more complex controls than a priori control, which only secures authentications and authorizations based on predefined roles [17]. This seems all the more important as the "Annex to the Commission Recommendation on a European Electronic Health Record exchange format" [18] provides that "any processing of health data should be registered and verified for auditing purposes, using appropriate techniques, such as logging and audit trailing, to keep an accurate record of the access to electronic records, their exchange or any other processing operation".

Such a control mechanism in large institutions seems audacious, but one can imagine a systematic monitoring of requests to open files (*recommended in point 2 of the previous section*) for those opened with a low recurrence (1 - 3 times), during a short period (1 second to 2 hours) and

by a single person. Monitoring could be carried out by the Data Protection Officer, following an automatic alert when the three above-mentioned conditions occur together and no other event concerning the case in question takes place within the next 7 days. With such a system, healthcare staff will no longer be able to abuse access since only the files used by their department will in principle be accessible to them.

Since technical staff have unlimited access, there must also be specific control. Although monitoring seems quite complicated (since these employees are in charge of managing the IT system), a report on 15% of activities randomly selected could provide a good overview of their activities. The Data Protection Officer would have to ensure that the activities correspond to specific IT requests and would also have to take a specific computer training course to understand and extract information on employee activities.

Additionally, in view of the sensitivity of medical information and the importance of its protection, we recommend that each national data protection authority should, as long as the law allows, carry out audits to observe the reality of the protection of patient information and monitor the work of the data protection officers [19].

In addition to these control measures, it seems necessary that the legal framework be changed in order to increase the awareness of the staff (*C*).

C. *A change in the legal framework for staff*

Raising awareness among medical professionals must be considered, as privacy respect is probably a major breach of data protection. The deployment of e-health systems will not be complete until professionals are correctly notified of their obligations. A cultural change must therefore be made in order to achieve the objective of data protection through the digitization of medical records. However, for change to happen, it is necessary to regulate individuals by law because without the threat of sanctions, it is practically certain that the situation will not change. According to the literature studied, in real life, this is often done using a bail sum or by some legally binding agreement, such as an employment contract [17].

When a new employee takes up his or her post, training should be provided on the importance of discretion and significant internal sanctions applied in the event of a breach. Each hospital should stipulate in its internal rules that employees with access to EMR are strictly bound to respect privacy. Such a general provision seems adequate to cover the weaknesses of the various data protection laws regarding non-medical personnel having access to the patient's electronic records.

In order to ensure a safe system, each medical establishment should require a written commitment to secrecy from doctors, auxiliaries, assistants and also technical and administrative staff. In Germany, it has been reported that medical records have been copied by computer scientists commissioned by a hospital to resell the data to the pharmaceutical industry. Increased caution should therefore be exercised with regard to these employees as soon as they take up their duties.

While this technical and legal framework offers more confidence in electronic records, we believe that the key to a safe system is the patient's own control of the record (*D*).

D. *Patient control of the file through technical measures*

At present, patients have no access to their electronic medical record, they can only have an extract when exercising their right of access to their personal data [20]. Existing solutions are insecure in terms of data protection because the patient has no view of the staff work and is totally passive. However, it has been found that patient access may not only lead to improved medical treatment, (for example, one patient discovered a brain tumor by exploring his data [21]), but it could also provide the patient with control over his/her personal medical record [22].

In the digital age, the demands for transparency towards data-holding entities are increasing. The simplest solution to meeting this obligation would therefore be to allow the patient to monitor his or her file. This is an important step in the management of electronic medical records but will require considerable amount of work since the software has not been designed in this way and will have to undergo significant changes.

1. First, visibility of access and documents should be provided to the patient:

This seems to be the most appropriate way to meet the challenges of security and data protection since it is the patient himself who will be responsible for issuing any complaints. Some doctors and writers are reluctant to accept such a possibility, however, since patients could as a result obtain information about the staff's perception of them [23]. This case is presented in particular with the doctor's personal notes. It is nevertheless perfectly normal that patients should have access to their personal data. The HUG preaches transparency and recommends that staff do not write anything down or if such remarks are on record that they do communicate them. In our view, in the name of transparency and the fact that this information concerns the lives of individuals, access should be allowed.

However, such a control system could reduce the veracity of medical information. Access to EMR should only be a reading and comment option, followed by the possibility to submit a wish for change to the Data Protection Officer in the event of undue access. Writing could be dangerous to the integrity of the data if the patient suffers from problems such as psychiatric disease and writes false information or if a child deletes the files. It is therefore necessary to implement a control solution, without the possibility of direct modification, which can only be made after discussion with a DPO. One option must then be created to request a modification, the DPO being permitted

to it online and change the information after a discussion with the doctor.

2. Allow direct access management:

The patient will be able to modify the options provided by the EMR and make adjustments to the permissions according to his preferences. The patient should also be able to exclude access to certain categories of people and more specifically, certain employees. Indeed, it seems obvious that certain specific information must be hidden from certain categories of employees or from a specifically named one. For example, an abortion is often an event about which a person is ashamed and has no bearing on other treatment, so a woman may wish to hide it from everyone except members of the gynecology department. The issue of patient access management is delicate for people who are not fully capable of discernment, but it is easy to imagine that a person in charge, such as parents in the case of a minor or a curator in the case of an adult, would exercise their rights in the interest of the person.

The questions that remains and that will require further study is how to technically implement and authenticate this patient control, how to choose a suitable platform and achieve balance between these general principles and the increasing use of electronic health records (EHR).

IV. CONCLUSION

Through this study, we proposed pragmatic recommendations with a fair balance between control and trust that ensures the continuity of hospital activities in an efficient manner. To find this balance we have observed that several factors must be taken into account: legal, technical and operational requirements. Control would not have been a valid solution for hospitals since information must flow freely for effective care, but neither total trust, since data protection rules do not allow free access for all. This makes it clear that technology alone cannot be the effective answer to a security problem, especially in complex and critical infrastructures such as hospitals. It should therefore be remembered that before implementing a technical security solution, all the needs of an organization must be taken into account. These can only be identified with an interdisciplinary collaborative approach. In the hospital context, this means that patients, medical or administration staff and lawyers' requirements must be integrated into the cybersecurity process, and that these people must work closely with security professionals.

REFERENCES

[1] 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).

[2] J. Oderkirk, J., "Readiness of electronic health record systems to contribute to national health information and research", OECD Health Working Papers, No. 99, OECD Publishing, Paris, (2017), Internet: https://doi.org/10.1787/9e296bf3-en, [August 9, 2019] .

[3] S. Sassi and C. Verdier, "Presentation and visualization of medical documents. The electronic medical record" (in French), Document numérique 2009/3, Vol. 12, 2009, pp. 37-58.

[4] Data protection and transparency officer of the Berne canton, "Patient records and data protection: what are your rights?" (in French), Internet:
https://www.jgk.be.ch/jgk/fr/index/aufsicht/datenschutz/gesundheit.assetref/dam/documents/JGK/DS/fr/DS_Broschuere_Patientendossier_en.pdf, Bern, 2015, [March 29, 2019].

[5] Federal Act on Data Protection (FADP) of 19 June 1992 (Status as of 1 March 2019); SR 235.1.

[6] D. Manaï, "Patient rights and biomedicine" (in French), 2nd ed., Stämpfli, Bern, 2013, p. 137.

[7] P. Meier, "Data Protection" (in French), Bern, 2011, p. 268.

[8] B. Birmele, B Bocquillon and R. Papon, "The electronic record: between data sharing for optimal patient care and the risk of breach of confidentiality" (in French), Médecine & droit, n°121, 2013, p. 140.

[9] M. Hirsig-Vouilloz, "The physician's responsibility" (in French), Stämpfli, Bern, 2017, p.194.

[10] D. Sprumont and S. Yvali, "Health law: the latest developments of the past year" (in French), Nouvelles technologies et santé publique - 22ème Journée de la santé, 3 septembre 2015, Weblaw, Bern, 2016, p. 5.

[11] Swiss Criminal Code of 21 December 1937 (Status as of 1 March 2019); SR 311.0.

[12] B. Corboz, "Offences in Swiss Law" (in French), Vol. 2, 3rd ed., Stämpfli, Bern, 2010, p. 759.

[13] A. Hertig Pea, "Is the protection of personal medical data effective?" (in French), Neuchâtel, Helbing Lichtenhahn, 2013, p. 86.

[14] M. Dupuis, L. Moreillon, C. Piguet,, S. Berger, M. Mazou and V. Rodigari, "A brief comment - Penal Code, book 2" (in French), 2nd ed., Helbing Lichtenhahn, Basel, 2017, p. 2025.

[15] D. Fabbri, K. LeFevre, "Explaining accesses to electronic medical records using diagnosis information", Journal of the American Medical Informatics Association, Volume 20, Issue 1, January 2013, Pages 52–60, Internet: https://doi.org/10.1136/amiajnl-2012-001018 [August 9, 2019].

[16] T. Sahama, L Simpson and B. Lane, "Security and Privacy in eHealth: is it possible", IEEE 15th International Conference on e-Health Networking, Applications and Services, Healthcom, 2013, p. 4.

[17] M. Dekker, S. Etalle, "Audit-Based Access Control for Electronic Health Records", Electr. Notes Theor. Comput. Sci.. 168. 221-236. 10.1016/j.entcs.2006.08.028, 2007.

[18] European Commission, " Annex to the Commission Recommendation on a European Electronic Health Record exchange format", C(2019)800) of 6 February 2019.

[19] J. S. Fernández-Alemán, I. Carrión Señor, P. A. O. Lozoya and A. Toval, "Security and privacy in electronic health records: A systematic literature review", Journal of Biomedical Informatics 46 (2013), p. 558.

[20] N. Innab, "Availability, accessibility, privacy and safety issues facing electronic medical records", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 7, No 1, February 2018, p. 7.

[21] S. Lohr, "The Healing Power of Your Own Medical Records", Internet: https://www.nytimes.com/2015/04/01/technology/the-healing-power-of-your-own-medical-data.html?referrer=&_r=2, March 31, 2015 [April 15, 2019].

[22] M. Smit, M. McAllister and J. Slonim, "Privacy of Electronic Health Records: Public Opinion and Practicalities", NAEC, 2005, p. 7.

[23] J. Wainer, C.J.R. Campos, M.D.U. Salinas and D. Sigulem, "Security requirements for a lifelong electronic health record system: an opinion", The open medical informatics journal, vol. 2, 2008, p. 162.