Australian Journal of Basic and Applied Sciences

2024; 18(4): pages 7-13
https://doi.org/10.22587/ajbas.2024.18.4.2

ORIGINAL ARTICLE AENSI Publications

Core impacts of patient data security

[*]Regina de Oliveira Benedito, [1]Pamela Nery do Lago, [1]Karine Alkmim Durães, [1]Gabriela Camargos Costa, [1]Divina Elenice Cardoso Bessas, [1]Lícia Caroline Bastos, [1]Renata Castro Mendes, [1]Luciana de Morais Lisboa, [1]Flávia de Oliveira Freitas, [1]Noel Morais de Souza, [1]Marilete Henrique Santiago Siqueira, [1]Tatiane Cristina de Castro Brito, [1]César de Faria Rezende, [1]Suellen Ferreira Santos Silva, [1]Bianca Cristina Silva Assis Santiago, [1]Taise Vieira Barros, [1]Ronaldo Gomes Rodrigues, [1]Letícia Maria de Oliveira Nogueira da Gama, [1]Ana Carolina Carvalho Rios, [1]Juliana da Silva Mata, [1]Priscila Costa Ribeiro Esteves, [1]Samira Alves Barbosa Gonçalves, [1]Iany Neres Ramalho, [1]Patrícia Gislene Dias, [1]Clarice Paraíso Ribeiro, [1]Maíra Amaral Silveira Gomes Ferreira, [1]Mariana de Oliveira Santos, [1]Andreia Christianne Lessa Souza, [2]Ana Kelly Alexandre Martins Soares, [2]Andrea Molina Lima Avelino, [2]Eveline Araújo Maia, [2]Maria Artunilda Bezerra Pinho, [2]Deisy Rejane Barbosa Bezerra, [2]Samanntha Lara da Silva Torres Anaisse, [3]Nayara Lummy Arashiro de Lima, [3]Cristiane de Oliveira Ribeiro, [3]Marta Luiza da Cruz, [4]Jéssica Laianne da Silva Carvalho, [4]Cicília Fernanda Pessoa Moura, [4]Francisca Áurea Portela Martins Carvalho, [4]Janielle Bandeira Melo, [4]Maracy Borges Xavier, [5]Samara Oliveira Lopes, [5]Kelly Franciane Lima Alves, [5]Grayce Kelly Nunes Fernandes, [5]Naiane dos Santos Campos Gama, [6]Juliane Guerra Golfetto, [7]Maria Auxiliadora Sena Conceição, [8]Tatiana Batista da Silva, [9]Lana Rose Cortez de Farias, [10]Bianca Ramalho dos Santos Silva, [11]Ayla Lima Soares, [12]Anna Elizabeth Grant de Oliveira, [13]Polyana Christine de Oliveira, [14]Diana de Oliveira Bezerra, [15]Lilian Maria Santos Silva, [16]Adriana Simões Moreira Rocha

[1]Clinical Hospital of the Federal University of Minas Gerais / Brazilian Hospital Services Company (HC-UFMG/EBSERH), Av. Prof. Alfredo Balena, 110, Santa Efigênia, 30130-100, Belo Horizonte, Minas Gerais, Brazil;
[2]Maternity School Assis Chateaubriand of the Federal University of Ceará / Brazilian Hospital Services Company (MEAC-UFC/EBSERH), Rua Coronel Nunes de Melo, s/n, Rodolfo Teófilo, 60430-270, Fortaleza, Ceará, Brazil;
[3]Maria Aparecida Pedrossian University Hospital of the Federal University of Mato Grosso do Sul / Brazilian Hospital Services Company (HUMAP-UFMS/EBSERH), Av. Sen. Filinto Müler, 355, Vila Ipiranga, 79080-190, Campo Grande, Mato Grosso do Sul, Brazil;
[4]University Hospital of the Federal University of Piauí / Brazilian Hospital Services Company (HU-UFPI/EBSERH), Campus Universitário Ministro Petrônio Portela, s/n, Ininga, 64049-550, Teresina, Piauí, Brazil;
[5]University Hospital of the Federal University of Sergipe / Brazilian Hospital Services Company (HU-UFS/EBSERH), R. Cláudio Batista - Dom Luciano, 49060-108, Aracaju, Sergipe, Brazil;
[6]University Hospital of the Federal University of Santa Maria / Brazilian Hospital Services Company (HUSM-UFSM/EBSERH), Av. Roraima, 1000, Camobi, 97105-900, Santa Maria, Rio Grande do Sul, Brazil;
[7]Professor Edgar Santos University Hospital of the Federal University of Bahia / Brazilian Hospital Services Company (HUPES-UFBA/EBSERH), R. Dr. Augusto Viana, s/n, Canela, 40110-060, Salvador, Bahia, Brazil;
[8]Presidente Dutra University Hospital / Brazilian Company of Hospital Services (HU-UFMA/EBSERH), R. Barão de Itapari, 227, Centro, 65020-070, São Luís, Maranhão, Brazil;
[9]Ana Bezerra University Hospital of the Federal University of Rio Grande do Norte (HUAB-UFRN/EBSERH), Praça Tequinha Farias, 13, 59200-000, Santa Cruz, Rio Grande do Norte, Brazil;
[10]Professor Alberto Antunes University Hospital of the Federal University of Alagoas / Brazilian Hospital Services Company (HUPAA-UFAL/EBSERH), Av. Lourival Melo Mota, S/N, Tabuleiro do Martins, 57072-900, Maceió, Alagoas, Brazil;
[11]Walter Cantídio University Hospital of the Federal University of Ceará / Brazilian Hospital Services Company (HUWC-UFC/EBSERH), R. Pastor Samuel Munguba, 1290, Rodolfo Teófilo, 60430-372, Fortaleza, Ceará, Brazil;
[12]Maternity School Januário Cicco of the Federal University of Rio Grande do Norte / Brazilian Hospital Services Company (MEJC-UFRN/EBSERH), Av. Nilo Peçanha, 259, Petrópolis, 59012-310, Natal, Rio Grande do Norte, Brazil;
[3]Nursing student at PUC Minas Coração Eucarístico, Av. Dom José Gaspar, 500, Coração Eucarístico, 30535-901, Belo Horizonte, Minas Gerais, Brazil;
[14]Clinical Hospital of the Federal University of Pernambuco / Brazilian Hospital Services Company (HC-UFPE/EBSERH), Av. Prof. Moraes Rego, 1235, Cidade Universitária, 50670-901, Recife, Pernambuco, Brazil;
[15]Gaffrée and Guinle University Hospital of the Federal University of the State of Rio de Janeiro / Brazilian Company of Hospital Services (HUGG-UNIRIO/EBSERH), R. Mariz e Barros, 775, Maracanã, 20270-004, Rio de Janeiro, Brazil;
[16]Climério de Oliveira Maternity Hospital of the Federal University of Bahia / Brazilian Company of Hospital Services (MCO-UFBA/EBSERH), R. do Limoeiro, 137, Nazaré, 40055-150, Salvador - Bahia, Brazil.

Australian Journal of Basic and Applied Sciences
ISSN: 1991-8178, EISSN: 2309-8414
Journal home page: www.ajbasweb.com

Correspondence Author:: Regina de Oliveira Benedito. Clinical Hospital of the Federal University of Minas Gerais / Brazilian Hospital Services Company (HC-UFMG/EBSERH), Av. Prof. Alfredo Balena, 110, Santa Efigênia, 30130-100, Belo Horizonte, Minas Gerais, Brazil.
E-mail: pamela.lago@ebserh.gov.br
ORCID: 0000-0002-3164-5165

Received date: 12 June 2024, Accepted date: 12 July 2024

ABSTRACT: Background: Records created by healthcare teams are intended to provide information about the care provided, ensure communication between team members and become a legal document for the defense of professionals and therefore must be imbued with authenticity and insignificance. The electronic medical record (EPR) is a technological resource that is increasingly used and should permanently replace the physical record. The security of EPR data is a concern for both the multidisciplinary care team and healthcare managers. Characterizing the extent of use of the EPR and confirming the effectiveness of data security mechanisms can support acceptance and compliance with the EPR by both healthcare professionals and administrative staff. Objective: Discuss the security of patient data using EPR in Brazil. Methodology: A literature review was conducted on this topic using bibliographic and descriptive research with a qualitative approach. The bibliographic survey was conducted electronically in the PUBMED and LILACS databases using the keywords: electronic medical record, data security, information technology. 23 scientific articles were analyzed, using as inclusion criteria articles published in Portuguese and English in the last ten years, complete and indexed in the above-mentioned databases. Results: Electronic medical record is the storage of clinical data from various sources, stored electronically to allow rapid and organized retrieval, with information about a group of patients or a specific patient. In order to prevent confidential information in the healthcare sector from being passed on without authorization, as is the case with patient files, especially electronic ones, secure information technology procedures must be used. With regard to the security of patient data, mechanisms must be in place to detect intrusions or unauthorized distribution of data and to impose strict sanctions on those who violate these mechanisms. Conclusion: It is believed that the certainty of severe punishment for non-compliance with information security and the right to privacy and confidentiality can significantly minimize these intrusions, thereby reducing resistance to compliance and acceptance of their use in everyday healthcare..

Keywords: ***Data protection. Electronic patient record. Health team.***

INTRODUCTION

The records created by the different categories of health professionals essentially serve to provide information about the assistance provided, to ensure communication between members of the health team and to become a legal document in defense of the professionals, and therefore must be authentic and legal meaning (Garcia; Ferreira; Silva, 2018). Patient development is a form of recording and therefore an important means of non-oral communication between multidisciplinary teams, academics and other professionals involved in the hospital context and outside the hospital context. Thus, an ethically carried out patient evolution consists of important legal resources and excellent educational materials for new research and training, thereby promoting the quality of care and user satisfaction (Silva; Areias, 2011).

In this context, attention to the quality and precision of procedures has been increasingly researched and studied. It is possible to see changes, nowadays, in a proactive and innovative way in this field. Following this path, Information Technology (IT) is being used as a major advance in the field of medical informatics. In recent decades, new applications, software and hardware have been implemented in medical and hospital processes, consolidating work standards and favoring the issue of precision and quality. Thus, currently, there are Electronic Medical Records, which apply Information Technology in the medical-hospital context. The Electronic Patient Record (EPR) is a technological resource that is increasingly used more frequently and should permanently replace the Physical Paper Record (PPR). The security of EPR data is a concern for both the multidisciplinary care team and managers. Characterizing the extent of use of the EPR and confirming the effectiveness of data security mechanisms can support acceptance and smoother adherence to the EPR by both healthcare and administrative professionals.

Patient data protection is a set of measures and practices that aim to ensure the confidentiality, integrity and availability of a patient's personal and health information. It is essential to guarantee the privacy and security of sensitive patient data, preventing unauthorized access, inappropriate use and potential privacy violations. Patient data protection is essential to ensure patients' trust in healthcare professionals and healthcare institutions, as well as to comply with data protection regulations and laws such as the General Data Protection Regulation (GDPR) in the European Union and the General Personal Data Protection Law (GPDPL) in Brazil (Governo Digital, 2020). Therefore, the objective of this article is to discuss the security of patient data using EPR in Brazil.

MATERIALS AND METHODS

This study consists of a literature review, using bibliographic and descriptive research as a basis, with a qualitative approach. Bibliographic material collected electronically was used in the Latin American and Caribbean Literature in Health Sciences (LILLACS) and PUBMED databases of the U.S. National Library of Medicine.

The search in the aforementioned databases took place between December 2023 and February 2024, using the following keywords: electronic patient record, data security, information technology.

23 scientific articles were analyzed using the following inclusion criteria: articles in Portuguese and English, complete, indexed in the aforementioned databases and that were similar to the theme of this study. After reading the articles, a new screening of the studies was carried out, confirming or not their relationship with the chosen topic. For data analysis, thematic grouping was proposed, based on the material acquired during reading. Finally, the data collected was analyzed for the development of the study and the elaboration of conclusions about it, establishing consonance with the substantiated objectives (Marconi; Lakatos, 2021).

RESULTS AND DISCUSSIONS

Medical records

The patient record or medical record is a physical or electronic document that contains relevant information about each patient and the care offered by the entire multidisciplinary health team, at the three levels of health care (Pinheiro *et al.*, 2016; Soares, 2016). It also serves to support research, teaching, management of health services, in addition to being a legal document for medical acts (Patrício *et al.*, 2011). Paper records are the most traditional forms and are subject to risks of breach of privacy and loss. Another difficulty in this type of medical record arises from the fact that over time large volumes of historical information, laboratory test results and diagnostic tests accumulate. Although it may be important for decision making, retrieving this information is quite laborious (Patrício *et al.*, 2011).

In the last 50 years, the first information systems based on electronic records emerged to establish internal communication between employees from different sectors. The programs and software currently available allow the storage of a large amount of data, which makes it easier to organize and process the information provided to the patient. In this way, health informatics can be useful for diagnoses, guidance and care provided to patients, as it enables a systematic analysis of their entire history, which favors more efficient decision-making among the different members of the healthcare team (Brasil, 2018a).

The electronic patient record

New technologies represent an important auxiliary tool for hospital management, allowing quick and hierarchical access to different organizational levels of data and information relating to patients, the quality of services provided, the human resources involved, productivity and other aspects related to suppliers (Parenzi, 2001; Wechsler, 2003; Furuie *et al.*, 2003).

For Lago et al. (2021): All of these health technologies have contributed to imaging studies, surgical procedures and various therapies, among others, and are proving promising in the near future, even in countries like Brazil, where there is still little government support and public institutions have few resources to research and develop more advanced technology projects. There are still long steps to be taken to reach the reality already observed in other countries, but yes, it is possible and fundamental to strive for this commitment and development in the health sector. Corroborating this idea, Santos *et al.* (2022) states that the EPR has become a crucial point both for establishing a connection with the patient and for improving the interpretation of health results, in addition to integrating planning teams with the expansion of information. This, consequently, helps in making better assertive decisions.

Under this perspective, Catarin (2023) points out that digital medical records represent a major technological advance in the health area, simplifying, speeding up and organizing case planning and allowing consistent storage of documents. Because it is digital, there is almost no problem with losing it and, combined with the encryption system, the exchange of these information between experts in different areas of the world is safe and efficient.

In the meantime, adding to the gains with the implementation of the EPR, which are countless, Nunes Junior, Silva and Magnagnagno (2021) prepared a comparison, seeking to highlight the advantages of the electronic medium (Table 1).

Table 1 - Comparison between Physical Paper Records (PPR) and Electronic Patient Record (EPR):

RECORDS	ADVANTAGES	DISADVANTAGES
Physical Paper Records (PPR)	- Greater freedom in the way of writing;	- Risks of damage or loss of the document;
	- Ease of handling;	- Illegibility due to difficult understanding of the handwriting by the healthcare team;
	- No training required to use it;	- Risk of erasure due to filling error
	- It is never "off air".	- Single space, territorialization;
		- Ambiguity;
		- Frequent loss of information;
		- Multiplicity of folders;
		- Difficulty in access and collective research;
		- Lack of standardization;
		- Paper fragility.
Electronic Patient Record (EPR)	- Can be easily shared between users and	- Limited to consultations in one place at a time;
	several professionals involved in patient care;	- Maintenance of EPR;
	- Can be consulted by different health institutions at the same time;	- Need for large investment in hardware, software and training;
	- Reduces service time and costs, eliminating redundancy in the demand for exams;	- Resistance to change;
	- Possibilities of historical and complete reconstruction of cases about patients, medical records, treatments, reports;	- Delay in implementation;
	- Contribution to research;	- Technology failures;
	- End of the problem of understanding ineligible letters;	- Failures in the electrical energy supply system;
	- Ease of organization and access to information;	- Depends on the speed of the Internet signal.
	- Rationality of large archiving space	
	quantities of documents;	
	- Communication between the patient and the healthcare team.	

Source: Nunes Junior, Silva e Magnagnagno (2021), Santos *et al.* (2022).

Seeking to minimize difficulties and resistance possibly presented by health teams, the Ministry of Health (MH) began a process of financial incentives and training for the implementation of EPR to replace PPR throughout the national territory since 2002:

The Electronic Patient Record emerged from the search for a system capable of integrating clinical and administrative information, with the main objective of optimizing and qualifying care, reducing costs and outlining the health profile of a region (Patrício, 2011, p. 67). Nunes Junior, Silva and Magnagnagno (2021) still discuss the issue, remembering that some currents in defense of paper records remain. However, the trend is towards total migration to electronic tools in health management, given the facilities introduced with such resources, in addition to security and capacity for data monitoring, as there are now federal laws established to protect the security of personal health information.

EPRs in the context of GPDPL

Law No. 13.709, of August 14, 2018, regulated the processing of personal data in Brazil, both in the public and private sectors (Brasil, 2018b). Known as the General Personal Data Protection Law (GPDPL), its provisions aim to protect the privacy of users and their personal data. To better understand the new law, Patrícia Peck Pinheiro, a specialist in digital law, states that: "The General Law for the Protection of Personal Data, Law No. 13.709/2018, is the Brazilian legislation that regulates personal data processing activities and that it also changes articles 7 and 16 of the Marco Civil da Internet" (Pinheiro, 2018, p. 37).

Even though Law No. 13.709/2018 emerged due to technological advances and influenced by the recently approved General Regulation on European Data Protection, the law did not only embrace digital media. The aforementioned law in the caput of its article 1 determines:

Art. 1. This Law provides for the processing of personal data, including in digital media, by natural persons or legal entities governed by public or private law, with the aim of protecting the fundamental rights of freedom and privacy and the free development of the personality of the natural person.

Even though data theft is sometimes reported as something that affects companies that operate over the Internet, the law also reached all other means, even physical and handwritten records, with no restrictions regarding its applicability to people and companies that operate online.
It is also noticeable the inclusion of health data in the list of "sensitive" data, which directly affects "hospitals, offices, health plans, laboratories, drugstores, etc." (Gouveia, 2018). Regarding what would be "data processing", there is item X of article 5 of Law No. 13.709/2018:

X. Treatment: All operation performed with personal data, such as those referring to collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, elimination, evaluation or control of information, modification, communication, transfer, diffusion or extraction. The fact is that there is a range of actions and possibilities, reaching various segments, even those that are not linked to the Internet. Therefore, every person/company that works with data from other people/companies needs to be in line with the GPDPL, regardless of the means of operation and the nature of their activity.

Invasion of privacy

Invasion of privacy, in general, concerns the collection and misuse of data. In this type of crime, people's data is collected, stored and distributed through easily accessible networks, without the person's knowledge or consent. According to Alexandre de Moraes, the constitutional guarantee of data confidentiality was inserted by the Federal Constitution of 1988 (Moraes, 2005). Thus, the inviolability of data secrecy is provided in article 5, XII, of the Federal Constitution and concerns the right to privacy, under the terms of the aforementioned provision: "the secrecy of correspondence and telegraphic communications, data and communications is inviolable. Telephone, except, in the last case, by court order, (...)";

Private life, that is, individual intimacy, in turn, finds protection in article 5, X, CF, which provides: "X - intimacy, private life, honor and image of people are inviolable, guaranteed the right to compensation for material or moral damage resulting from its violation;".

The caput of article 11 of Law No. 12.965/2014 (Civil Framework Law) deals with the storage and protection of personal data and the secrecy of communications:

Art. 11. In any operation of collection, storage, custody and processing of records, personal data or communications by connection providers and internet applications in which at least one of these acts occurs in national territory, the following must be compulsorily respected: Brazilian legislation and the rights to privacy, protection of personal data and the confidentiality of private communications and records.

Complementing the above, Brito (2022) states that: "Confidentiality in healthcare is a necessary tool to protect the patient's privacy and individuality, and the breach of this right can lead to a violation of fundamental rights and also human rights".
However, a considerable part of users still distrust encrypted applications. There are those who advocate leaving for certain networks that ensure user privacy.

Pinho (2000, p. 101) explains that the right to privacy, in the Federal Constitution of 1988, is found in the protection of intimacy, private life, honor and image of people. The author notes that: "Due to technological advances, with the increasing possibility of intrusion into people's intimate lives, it is essential to ensure, among individual rights, respect for the privacy of each human being".

Atheniense (2010) observes that it is necessary to be aware that the more technology advances, the more the devastation of privacy occurs, stating the author that the risk caused by technology cannot be seen as a lack of protection of Brazilian law, as there is already plenty of jurisprudence and legislation on the subject to inhibit abuses that may be committed against the honor of people and companies in virtual media. However, "it is very important to create the habit of monitoring the dissemination of texts, images, videos so that it is possible to quickly identify illicit content with a view to immediately removing it from circulation as a way of minimizing damage".

Pinho (2003, p. 101) understands that the right to privacy, within the system defined by the Federal Constitution, is a generic denomination where it is included in the protection of other fundamental rights of people. For the author, "due to technological advances, with the increasing possibility of intrusion into people's intimate lives, it is essential to ensure, among individual rights, respect for the privacy of each human being".

In this way, the leakage of confidential information without authorization in the healthcare area, such as patient records, especially electronic ones, must use secure IT processes, informing doctors, nursing staff and others, of the laws and regulations on the security of personal data.

CONTRIBUTION TO KNOWLEDGE

For EPR to be useful, it requires the adoption of standards in the representation of information, in the means of storing and exchanging information. And there must be an even greater concern: guaranteeing the patient freedom of access to their clinical history data, as the medical record belongs to the patient and not the healthcare team. However, for it to become a reality in Brazil, it is necessary to listen to and understand the main users of the systems, the health professionals, since their resistance is one of the factors that hinder the adoption of EPR.

CONCLUSION

The electronic medical record should be understood as the repository of clinical data obtained from various sources, stored electronically in order to allow quick and organized retrieval, with information from a group of patients or about a particular patient. Regarding the security of patient data, there must be mechanisms for detecting intrusion or dissemination of data without authorization, in addition to imposing severe sanctions for those who violate such mechanisms. It is believed that the certainty of severe punishment for non-compliance with information security and the right to privacy and confidentiality can greatly minimize these invasions. Protecting patient data is important to guarantee the quality of care, facilitate communication between healthcare professionals and ensure continuity of care. In summary, patient data protection seeks to protect the privacy and security of patients' personal and health information, ensuring their rights and promoting trust in the healthcare system.

CONFLICT OF INTEREST

As the authors of this manuscript, we certify that we have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in the manuscript.

COMPETING INTERESTS

None: There is no competing interests.

ETHICS COMMITTEE

None.

FUNDING INFORMATION

The work presented here has been privately funded.

AUTHORSHIP CONTRIBUTIONS

The authors of this publication develop it under the following main aspects:
1. Regina de Oliveira Benedito, Pamela Nery do Lago, Juliana da Silva Mata, Priscila Costa Ribeiro Esteves, Samira Alves Barbosa Gonçalves, Iany Neres Ramalho, Patrícia Gislene Dias, Clarice Paraíso Ribeiro, Maíra Amaral Silveira Gomes Ferreira, Mariana de Oliveira Santos, Andreia Christianne Lessa Souza, Ana Kelly Alexandre Martins Soares, Andrea Molina Lima Avelino, Eveline Araújo Maia: supported research planning and collection, as well as data analysis.
2. Pamela Nery do Lago, Maria Artunilda Bezerra Pinho, Deisy Rejane Barbosa Bezerra, Samanntha Lara da Silva Torres Anaisse, Nayara Lummy Arashiro de Lima, Cristiane de Oliveira Ribeiro, Marta Luiza da Cruz, Jéssica Laianne da Silva Carvalho: supported the writing of the article.
3. Regina de Oliveira Benedito, Pamela Nery do Lago, Karine Alkmim Durães, Gabriela Camargos Costa, Divina Elenice Cardoso Bessas, Lícia Caroline Bastos, Renata Castro Mendes, Luciana de Morais Lisboa, Flávia de Oliveira Freitas, Noel Morais de Souza: work advisors, supported in planning the study, guided data collection and data analysis and writing of the article.
4. Tatiane Cristina de Castro Brito, César de Faria Rezende, Suellen Ferreira Santos Silva, Bianca Cristina Silva Assis Santiago: participated in the interpretation and analysis of the data obtained and writing of the article.
5. Marilete Henrique Santiago Siqueira, Taise Vieira Barros, Ronaldo Gomes Rodrigues, Letícia Maria de Oliveira Nogueira da Gama, Ana Carolina Carvalho Rios: worked on the interpretation of the data obtained and final writing of the article.
6. Samara Oliveira Lopes, Kelly Franciane Lima Alves, Grayce Kelly Nunes Fernandes, Naiane dos Santos Campos Gama, Juliane Guerra Golfetto, Maria Auxiliadora Sena Conceição, Tatiana Batista da Silva, Lana Rose Cortez de Farias, Bianca Ramalho dos Santos Silva, Ayla Lima Soares, Anna Elizabeth Grant de Oliveira, Polyana Christine de Oliveira, Diana de Oliveira Bezerra, Lilian Maria Santos Silva, Adriana Simões Moreira Rocha: supported the final writing of the article.
7. Regina de Oliveira Benedito, Pamela Nery do Lago, Cicília Fernanda Pessoa Moura, Francisca Áurea Portela Martins Carvalho, Janielle Bandeira Melo, Maracy Borges Xavier: support in final writing and text corrections.

REFERENCES

Atheniense, A. 2010. A fragilidade da privacidade na era digital. In: Âmbito Jurídico. Available from: http://ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=7967&revista_caderno=17.

Brasil. 2018a. Ministério da Saúde, Secretaria de Atenção à Saúde. e-SUS Atenção Básica: Manual de uso do Sistema com Prontuário Eletrônico do Cidadão PEC - Versão 3.1. Brasília, DF: Ministério da Saúde.

Brasil. 2018b. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Available from: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

Brito, T. O. 2022. Direito do paciente à confidencialidade dos seus dados pessoais e a lei geral de proteção de dados pessoais. Trabalho de Conclusão de Curso (Graduação). Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília (UniCEUB), Brasília.

Catarin, J. P. (2023). Prontuário eletrônico – discussão dos aspectos fundamentais e as suas implicações no contexto odontológico atual. Trabalho de Conclusão de Curso (Graduação). Faculdade de Odontologia de Araçatuba, Universidade Estadual Paulista, Araçatuba.

Furuie, S. S. *et al.* 2003. Prontuário eletrônico de pacientes: integrando informações clínicas e imagens médicas. Rev. Bras. Eng. Biomed, 19 (3), 125-137.

Garcia, T. T., Ferreira, W. F. S. And Silva, A. 2018. Processo de auditoria em enfermagem e suas dimensões na assistência ao paciente: uma revisão sistemática de literatura. Rev. Ciência & Desenvolvimento-Eletrônica da FAINOR, 11 (1).

Gouveia, F. 2018. Lei de proteção de dados não é apenas para empresas que atuam on-line. Available from: https://www.conjur.com.br/2018-ago-17/fernando-gouveia-lei-dados-nao-quem-atua-on-line.

Governo Digital. 2020. Lei Geral de Proteção de Dados (LGPD): Guia de Boas Práticas para Implementação na Administração Pública Federal. Available from: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf.

Lago, P. N. *et al.* (2021). Como os avanços tecnológicos modificaram a dinâmica na saúde. International Journal of Development Research, 11 (12), 52816-52818. DOI: https://doi.org/10.37118/ijdr.23576.12.2021.

Marconi, M. A., Lakatos, E. M. 2021. Fundamentos de Metodologia Científica. Atlas. 9ª ed., Atlas, 368p.

Moraes, A. 2005. Direito Constitucional. 18. ed. São Paulo: Atlas.

Nunes Junior, J. F., Silva, D. L. and Magnagnagno, O. 2021. Análise comparativa dos prontuários eletrônico e físico sobre a segurança das informações. Fag Journal Of Health (FJH), 3 (2), 177-181. DOI: https://doi.org/10.35984/fjh.v3i2.307.

Parenzi, A. O. 2010. Auditoria funcional. Apostila do Curso de Pós-graduação da Universidade UNIMED em Auditoria da Saúde.

Patrício, C. M., Machiavelli, J. L., Maia, M. M., Navaes, M. A. 2011. O prontuário eletrônico do paciente no sistema de saúde brasileiro: uma realidade para os médicos? Scientia Medica, 21 (3), 121- 131.

Pinheiro, A. L. S., Andrade, K. T. S., Silva, D. O., Zacharias, F. C. M., Gomide, M. F. S. and Pinto, I. C. 2016. Gestão da Saúde: o uso dos sistemas de informação e o compartilhamento de conhecimento para a tomada e decisão. Texto Contexto Enferm., 25 (3): e3440015. DOI: https://doi.org/10.1590/0104-07072016003440015.

Pinheiro, P. P. 2018. Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018: LGPD. São Paulo: Saraiva.

Pinho, J. B. 2000. Publicidade e Vendas na Internet. São Paulo: Summus.

Pinho, R. C. R. 2003. Teoria geral da Constituição e direitos fundamentais. 4. ed. São Paulo: Saraiva.

Santos, É. R., Pereira, J. L., Finicelli, L. D. P., Costa, M. D. S. and Checchi, M. H. R. 2022. A utilização do Prontuário Eletrônico: um relato de experiência pelo olhar de estudantes de Medicina no interior do Amazonas. JMPHC | Journal of Management & Primary Health Care, 14, e003. DOI: https://doi.org/10.14295/jmphc.v14.1178.

Silva, N. P. and Areias, M. A. C. 2011. A importância das anotações de enfermagem no contexto econômico hospitalar. Available from: https://semanaacademica.org.br/system/files/artigos/aimportanciadasanotacoesdeenf.

Soares, E. V. B. 2016. Atenção Básica e Informação: análise do Sistema de Informação em Saúde para Atenção Básica (SISAB) e estratégia e-SUS AB e suas repercussões para uma gestão da saúde com transparência. Dissertação. (Trabalho de Conclusão de Curso). Universidade de Brasília, Brasília, DF.

Wechsler R., Anção, M. S., Campos, C. J. R., Sigulem, D. 2003. A informática no consultório médico. Jornal de Pediatria, 79, (Supl. 1), S3-S12. DOI: 0021-7557/03/79-Supl.1/S3

Citation: Regina de Oliveira Benedito, Pamela Nery do Lago, Karine Alkmim Durães, Gabriela Camargos Costa, Divina Elenice Cardoso Bessas, Lícia Caroline Bastos, Renata Castro Mendes, Luciana de Morais Lisboa, Flávia de Oliveira Freitas, Noel Morais de Souza, Marilete Henrique Santiago Siqueira, Tatiane Cristina de Castro Brito, César de Faria Rezende, Suellen Ferreira Santos Silva, Bianca Cristina Silva Assis Santiago, Taise Vieira Barros, Ronaldo Gomes Rodrigues, Letícia Maria de Oliveira Nogueira da Gama, Ana Carolina Carvalho Rios, Juliana da Silva Mata, Priscila Costa Ribeiro Esteves, Samira Alves Barbosa Gonçalves, Iany Neres Ramalho, Patrícia Gislene Dias, Clarice Paraíso Ribeiro, Maíra Amaral Silveira Gomes Ferreira, Mariana de Oliveira Santos, Andreia Christianne Lessa Souza, Ana Kelly Alexandre Martins Soares, Andrea Molina Lima Avelino, Eveline Araújo Maia, Maria Artunilda Bezerra Pinho, Deisy Rejane Barbosa Bezerra, Samanntha Lara da Silva Torres Anaisse, Nayara Lummy Arashiro de Lima, Cristiane de Oliveira Ribeiro, Marta Luiza da Cruz, Jéssica Laianne da Silva Carvalho, Cicília Fernanda Pessoa Moura, Francisca Áurea Portela Martins Carvalho, Janielle Bandeira Melo, Maracy Borges Xavier, Samara Oliveira Lopes, Kelly Franciane Lima Alves, Grayce Kelly Nunes Fernandes, Naiane dos Santos Campos Gama, Juliane Guerra Golfetto, Maria Auxiliadora Sena Conceição, Tatiana Batista da Silva, Lana Rose Cortez de Farias, Bianca Ramalho dos Santos Silva, Ayla Lima Soares, Anna Elizabeth Grant de Oliveira, Polyana Christine de Oliveira, Diana de Oliveira Bezerra, Lilian Maria Santos Silva, Adriana Simões Moreira Rocha.,2024. Core impacts of patient data security. Australian Journal of Basic and Applied Sciences, 18(4): 7-13. https://doi.org/10.22587/ajbas.2024.18.4.2.