


**INFORMATION SECURITY IN DIGITAL HEALTH IN THE POSTOPERATIVE PERIOD:
RISKS, LEGISLATION AND ETHICAL PRACTICES**

**SEGURANÇA DA INFORMAÇÃO EM SAÚDE DIGITAL NO PÓS-OPERATÓRIO:
RISCOS, LEGISLAÇÃO E PRÁTICAS ÉTICAS**

**SEGURIDAD DE LA INFORMACIÓN EN SALUD DIGITAL EN EL POSTOPERATORIO:
RIESGOS, LEGISLACIÓN Y PRÁCTICAS ÉTICAS**

 <https://doi.org/10.56238/sevened2025.031-011>

Rafael Alves Freires¹, Leonardo Gomes de Sousa², Jackson Roberto Sousa de Oliveira³, Anderson Daniel Viana Pantoja⁴, Camila Ferreira Alves⁵, Brenda Caroline de Andrade Camelo⁶, Juliana da Costa Furtado⁷, Aracélia Vieira da Silva⁸, Wanderson Alexandre da Silva Quinto⁹

ABSTRACT

Advances in digital health technologies have significantly transformed care delivery, especially in the postoperative period, by enabling remote patient monitoring, continuous communication between professionals and patients, and increased adherence to therapeutic approaches. However, these same advances introduce significant risks related to information security and the privacy of sensitive data, requiring increased attention from managers, professionals, and system developers. This article conducts an integrative review that examines the main cyber risks associated with digital postoperative care, the applicable legal provisions, with an emphasis on the General Data Protection Law (LGPD) and the European Union's General Data Protection Regulation (GDPR), and the ethical dilemmas that emerge from the use of digital technologies in clinical settings. The analysis also includes bioethical guidelines that guide professional practice in the digital age. The results highlight the urgent need to implement cybersecurity policies, continue training healthcare teams, strengthen informed consent, and promote an organizational culture focused on data protection. It is concluded that the humanization of care in digital environments is intrinsically linked to information ethics and the responsible protection of patient data. It is also concluded that teachers' persistence, integrity, and adaptability directly influence the ability to thematically address the content. This is possible through the adaptation of the materials required for

¹ Dentist. Master's Student in Surgery and Experimental Research. Universidade do Estado do Pará (UEPA), Brazil. E-mail: dr.rafael.freires22@gmail.com

² Nurse. Master's Student in Surgery and Experimental Research. Universidade do Estado do Pará (UEPA), Brazil. E-mail: leonardocantao13@gmail.com

³ Physiotherapist. Master's Student in Surgery and Experimental Research. Universidade do Estado do Pará (UEPA), Brazil. E-mail: jack.roberto21@gmail.com

⁴ Nurse. Master's Student in Surgery and Experimental Research. Universidade do Estado do Pará (UEPA), Brazil. E-mail: andersondvpantoja@hotmail.com

⁵ Physiotherapist. Master's Student in Surgery and Experimental Research. Universidade do Estado do Pará (UEPA), Brazil. E-mail: camila.ferreiraalves01@gmail.com

⁶ Nurse. Master's Student in Surgery and Experimental Research. Universidade do Estado do Pará (UEPA), Brazil. E-mail: brendacameloo@hotmail.com

⁷ Nurse. Master's Student in Surgery and Experimental Research. Universidade do Estado do Pará (UEPA), Brazil. E-mail: enf.julianafurtado@outlook.com

⁸ Lawyer. Master's Student in Surgery and Experimental Research. Universidade do Estado do Pará (UEPA), Brazil. E-mail: vieira-advocacia2011@hotmail.com

⁹ Professor. Doctor in Psychology. Master in Electrical Engineering. Universidade do Estado do Pará (UEPA), Brazil. E-mail: w.quinto@uepa.br

practice, the school space and/or surroundings where the activities will take place, and the pursuit of overcoming deficiencies in initial training, whether through continuing education and/or joint research and knowledge sharing, as emphasized by the participants.

Keywords: Information Security. Digital Health. Postoperative Care. LGPD. Bioethics. Privacy.

RESUMO

O avanço das tecnologias em saúde digital tem promovido transformações significativas na prestação de cuidados, especialmente no período pós-operatório, ao viabilizar o monitoramento remoto de pacientes, a comunicação contínua entre profissionais e usuários, e o aumento da adesão às condutas terapêuticas. No entanto, esses mesmos avanços introduzem riscos relevantes relacionados à segurança da informação e à privacidade de dados sensíveis, exigindo atenção redobrada de gestores, profissionais e desenvolvedores de sistemas. Este artigo realiza uma revisão integrativa que examina os principais riscos cibernéticos associados ao cuidado digital no pós-operatório, os dispositivos legais aplicáveis, com ênfase na Lei Geral de Proteção de Dados (LGPD) e no Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), e os dilemas éticos que emergem da utilização de tecnologias digitais em contextos clínicos. A análise inclui ainda diretrizes bioéticas que orientam a prática profissional na era digital. Os resultados destacam a urgência de implementação de políticas de cibersegurança, capacitação continuada das equipes de saúde, fortalecimento do consentimento informado e promoção de uma cultura organizacional voltada à proteção de dados. Conclui-se que a humanização do cuidado em ambientes digitais está intrinsecamente ligada à ética da informação e à proteção responsável dos dados dos pacientes. -se que a persistência, a seriedade e a capacidade de adaptação e de superação dos docentes influencia diretamente na possibilidade de tematização do conteúdo, sendo isto possível por meio da adaptação dos materiais necessários para a prática, do espaço escolar e/ou proximidades onde se desenvolverão as atividades, e da busca pela superação da deficiência na formação inicial, quer seja por intermédio da formação continuada e/ou pela pesquisa e compartilhamento conjuntos de conhecimentos, conforme enfatizado pelos pesquisados.

Palavras-chave: Segurança da Informação. Saúde Digital. Cuidados Pós-Operatórios. LGPD. Bioética. Privacidade.

RESUMEN

Los avances en las tecnologías de salud digital han transformado significativamente la prestación de servicios de salud, especialmente en el período postoperatorio, al permitir la monitorización remota de pacientes, la comunicación continua entre profesionales y pacientes, y una mayor adherencia a los enfoques terapéuticos. Sin embargo, estos mismos avances introducen riesgos significativos relacionados con la seguridad de la información y la privacidad de datos sensibles, lo que requiere una mayor atención por parte de gestores, profesionales y desarrolladores de sistemas. Este artículo realiza una revisión integrativa que examina los principales riesgos cibernéticos asociados a la atención postoperatoria digital, las disposiciones legales aplicables, con énfasis en la Ley General de Protección de Datos (LGPD) y el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, y los dilemas éticos que surgen del uso de tecnologías digitales en entornos clínicos. El análisis también incluye directrices bioéticas que guían la práctica profesional en la era digital. Los resultados destacan la urgente necesidad de implementar políticas de

ciberseguridad, continuar la formación de los equipos sanitarios, fortalecer el consentimiento informado y promover una cultura organizacional centrada en la protección de datos. Se concluye que la humanización de la atención en entornos digitales está intrínsecamente ligada a la ética de la información y a la protección responsable de los datos de los pacientes. También se concluye que la persistencia, integridad y adaptabilidad del profesorado influyen directamente en la capacidad de abordar temáticamente el contenido. Esto es posible mediante la adaptación de los materiales necesarios para la práctica, el espacio escolar y/o el entorno donde se desarrollarán las actividades, y la búsqueda de soluciones para las deficiencias en la formación inicial, ya sea mediante la formación continua y/o la investigación conjunta y el intercambio de conocimientos, como destacaron los participantes.

Palabras clave: Seguridad de la Información. Salud Digital. Cuidados Postoperatorios. LGPD. Bioética. Privacidad.

1 INTRODUCTION

The growing digitalization of health services, catalyzed by the advancement of information and communication technologies, has promoted significant transformations in the way health care is offered, especially in the postoperative context. Resources such as mobile applications aimed at health, telemedicine platforms, electronic medical record systems, and remote monitoring devices have started to play a central role in the clinical follow-up of patients after surgical procedures. These tools allow the continuous sending of physiological data, such as body temperature, heart rate, and blood pressure, as well as the recording of symptoms, facilitating closer clinical surveillance, even from a distance. In addition, they enable faster and more efficient communication between patients and health professionals, which can favor early interventions in the face of signs of complications. This new logic of care enhances the continuity of care, promotes greater autonomy for the patient, and contributes to the reduction of unnecessary hospital admissions.

However, the integration of digital information flows into postoperative care also poses considerable challenges, especially with regard to information security and the protection of individuals' privacy. The digital environment, while offering operational facilities, can become a vulnerable space, exposed to risks such as leakage of sensitive data, unauthorized access, misuse of clinical information, and failures in authentication systems. Such incidents compromise not only the confidentiality of information, but also the relationship of trust between patients and institutions, and can generate irreparable ethical, legal and psychological damage.

In view of this scenario, this article aims to develop an integrative and in-depth analysis of information security in the context of digital health aimed at postoperative care. The investigation focuses on the identification and categorization of the main digital risks associated with the use of technologies in the post-surgical phase, as well as on the review of the applicable regulatory frameworks, with emphasis on the General Data Protection Law (LGPD), in force in Brazil, and the General Data Protection Regulation (GDPR), in force in the European Union. In addition, the ethical implications arising from the adoption of these technologies are discussed, both for health professionals, who must ensure conduct guided by confidentiality and respect for informed consent, and for institutions, which have the legal and moral responsibility to protect user data in the face of threats from the digital environment. It is, therefore, a reflection that seeks to articulate the technical, legal and ethical aspects

related to the protection of sensitive data in a context of increasing computerization of health services.

2 METHODOLOGY

This is an integrative literature review study, whose objective was to gather, analyze and critically synthesize scientific productions, legal documents and relevant technical-normative guidelines on information security in the context of digital health applied to postoperative care. Data collection was carried out between April and July 2025, including publications available in the period from 2015 to 2025. For the systematized search, national and international scientific databases were used, including PubMed, Scopus, SciELO, LILACS and Google Scholar, as well as specialized legal repositories, such as Jusbrasil and LegisWeb.

The following descriptors and combined terms were used, in Portuguese, English and Spanish, according to the DeCS/MeSH controlled vocabulary: "information security", "digital health", "postoperative", "bioethics", "LGPD", "privacy", and "health data protection". The search strategy used Boolean operators (AND, OR) for greater accuracy in the retrieval of sources.

The inclusion criteria included: (i) scientific articles published in peer-reviewed journals; (ii) normative and legal documents with recognized applicability in the field of digital health; (iii) texts written in Portuguese, English or Spanish; and (iv) publications that demonstrate thematic relevance, topicality, and proven scientific relevance. Duplicate studies, abstracts without full text, unsubstantiated opinions, or publications that did not directly address the proposed thematic focus were excluded.

Data selection, extraction, and analysis were performed independently by two reviewers, following a systematic approach to ensure the consistency and quality of the integrative synthesis.

3 DIGITAL HEALTH IN THE POSTOPERATIVE PERIOD

The use of technology in postoperative follow-up has allowed for a more effective and patient-centered approach. Mobile devices, vital signs monitoring apps, teleconsultation platforms, and interoperable electronic medical records have been used to track recoveries, avoid complications, ensure medication adherence, and offer psychosocial support.

However, this new scenario also exposes sensitive data to risks such as leaks in connection nodes (over public Wi-Fi, for example), authentication failures, use of unprotected personal devices (BYOD - Bring Your Own Device), among others.

4 CYBER RISKS IN THE POSTOPERATIVE CONTEXT

The main digital risks identified in the literature include:

- Theft of personal and health data;
- Information hijacking by ransomware;
- Improper manipulation of medical records;
- Use of sensitive information for commercial or discriminatory purposes;
- Lack of adequate digital consent.

Emblematic cases, such as the cyberattack that occurred in 2021 against one of the largest health plan operators in Brazil, strongly highlight the vulnerability of information structures in the health sector in the face of cyber threats. These episodes reveal not only the technical weaknesses of the systems, but also the insufficiency of robust prevention, response and mitigation policies. The consequences are severe and immediate, directly affecting the confidentiality, integrity, and availability of sensitive patient data, in addition to compromising public trust in the institutions responsible for care management.

5 APPLICABLE LEGISLATION: LGPD AND GDPR

The General Law for the Protection of Personal Data (LGPD – Law No. 13,709/2018) establishes principles and guidelines for the processing of personal data in Brazil, expressly including the health sector. According to the legislation, health-related data is classified as sensitive data, which implies the adoption of additional safeguards, such as specific consent, stricter security measures, and restrictions on unauthorized sharing. Similarly, the General Data Protection Regulation (GDPR), in force in the European Union since 2018, incorporates fundamental concepts such as explicit consent, purpose limitation, data minimization, and the principle of accountability.

Both regulations impose clear and detailed obligations on healthcare institutions regarding the complete cycle of digital data — from collection and storage to sharing and disposal. Such legislation requires processing agents to adopt technical and organizational measures appropriate to the nature of the data processed, ensuring not only the security of

the information, but also transparency and the protection of the rights of the data subjects. In a scenario of increasing digitalization of health care, alignment with the provisions of the LGPD and GDPR is an ethical, legal, and operational imperative.

6 ETHICAL ASPECTS OF HEALTH INFORMATION PROTECTION

Bioethics applied to the context of digital health invites a critical reinterpretation of the fundamental principles of beneficence, non-maleficence, autonomy and justice, in the face of the challenges imposed by emerging technologies. In scenarios marked by the massive collection, storage, and sharing of sensitive data, the protection of privacy is no longer just a technical obligation and becomes an essential ethical right, directly linked to the patient's autonomy. Ensuring this autonomy implies ensuring a robust, clear, and contextualized informed consent process, especially in digital environments, where risks are often invisible to the user and decisions are mediated by algorithms. Thus, digital ethics in health requires practices that reconcile innovation with responsibility, ensuring that technological advances are always at the service of human dignity.

Practices should consider:

- Transparency in the use of data;
- Limitation of access by professionals;
- Audit and traceability logs;
- Ethics in the use of AI and algorithms in postoperative follow-up.

7 GOOD INFORMATION SECURITY PRACTICES

Effective information protection involves technical and organizational actions:

- Encryption of data at rest and in transit;
- Multi-factor authentication (MFA);
- Regular backups;
- Training of teams on cybersecurity and digital ethics;
- Periodic audits and vulnerability management.

8 DISCUSSION

Contemporary literature shows a permanent tension between the advancement of technological innovations applied to health and the need to ensure the ethical and legal protection of sensitive patient data. On the one hand, the digital resources used in postoperative care, such as monitoring applications, communication platforms, and electronic medical record systems, promote significant improvements in efficiency, continuity of care, and personalization of treatment. On the other hand, the accelerated implementation of these technologies, often without proper investment in cybersecurity and without the consolidation of an organizational culture focused on data protection, has exposed institutions and individuals to critical vulnerabilities.

Studies show that the fragility of health information systems, associated with the absence of robust security protocols and the lack of continuous training for teams, increases the risks of privacy violations, misuse of data, and breach of confidentiality of the fundamental principles of bioethics. In many organizations, especially in the public sector and in services with limited infrastructure, data protection is still not treated as a strategic priority, which compromises user trust and exposes professionals to ethical and legal dilemmas.

In this scenario, digital health information governance assumes a central role. Institutions are required to adopt integrated information security policies, based not only on compliance with legal requirements, such as the General Data Protection Law (LGPD) in Brazil and the General Data Protection Regulation (GDPR) in the European Union, but also on the ethical principles of beneficence, autonomy, justice, and non-maleficence. Adherence to international protocols of good practices in cybersecurity, strengthening informed consent in digital environments, and promoting continuing education in digital ethics are fundamental strategies to mitigate risks and ensure the integrity of care.

Therefore, overcoming this apparent paradox between innovation and protection depends on the recognition that information security is not an obstacle to modernization, but an essential pillar for its legitimacy and sustainability. The contemporary challenge is to align technological advances with ethical, transparent, and patient-centered governance, ensuring that the humanization of care is also expressed in the responsible protection of data in digital environments.

9 FINAL CONSIDERATIONS

Information security in the field of digital health, especially in the postoperative context, must be understood beyond a merely technical or legal requirement. It is an essential component of an ethical, safe and truly patient-centered practice. The integrity and confidentiality of sensitive data not only sustain trust between users and health professionals, but also represent fundamental guarantees of the bioethical principles of autonomy, beneficence and justice.

Protecting patient data is ensuring that your personal and clinical information is used transparently, responsibly and respectfully, contributing to safer clinical decisions and stronger therapeutic relationships. In the contemporary scenario, where digital care is becoming increasingly present and comprehensive, neglecting data protection is equivalent to weakening citizens' rights and compromising the legitimacy of health technologies.

In this sense, the construction of an institutional culture guided by digital ethics is imperative. It requires the strengthening of information governance policies, continuous investments in cybersecurity, qualification of multidisciplinary teams, and expansion of the public debate on patients' rights in digital environments. It is concluded, therefore, that the humanization of care in the twenty-first century involves, unavoidably, the consolidation of practices that reconcile technological innovation with ethical responsibility and commitment to the protection of human dignity.

REFERENCES

- Agência Nacional de Saúde Suplementar. (2022). Diretrizes de segurança da informação para operadoras. Brasília, Brazil: ANS.
- Brasil. (2018). Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União. Retrieved from http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
- Brasil. Autoridade Nacional de Proteção de Dados. (2021). Guia orientativo para agentes de tratamento de pequeno porte. Brasília, Brazil: ANPD.
- Conselho Nacional de Justiça. (2023). Diretrizes de LGPD no Judiciário. Brasília, Brazil: CNJ.
- Dias, L. M., et al. (2022). Cibersegurança em sistemas de saúde: Uma revisão integrativa. *Revista Brasileira de Enfermagem*, 75(3), e20210456. <https://doi.org/10.1590/0034-7167-2021-0456>
- Fernandes, P. H., et al. (2020). Uso de aplicativos em pós-operatório e segurança da informação. *Journal of Health Informatics*, 12(4), 123–130.

- Ferreira, J. R., & Luz, T. C. (2019). Riscos digitais em ambientes hospitalares. *Informática em Saúde*, 11(2), 45–52.
- Greenhalgh, T., et al. (2021). Digital health and the ethics of care. *The Lancet Digital Health*, 3(6), e352–e359. [https://doi.org/10.1016/S2589-7500\(21\)00062-4](https://doi.org/10.1016/S2589-7500(21)00062-4)
- International Organization for Standardization. (2013). *ISO/IEC 27001: Information security management systems*. Geneva, Switzerland: ISO.
- Kluge, E.-H. W. (2016). Ethical and legal challenges for health telematics. *Studies in Health Technology and Informatics*, 225, 12–16. <https://doi.org/10.3233/978-1-61499-664-4-12>
- Lopes, F. C., & Ramos, M. (2020). Bioética e proteção de dados em saúde. *Interface*, 24, e190567. <https://doi.org/10.1590/interface.190567>
- Luna, F. (2020). Privacy and vulnerability in digital health. *Journal of Medical Ethics*, 46(12), 794–799. <https://doi.org/10.1136/medethics-2020-106151>
- Mendes, K. D. S., et al. (2016). Revisão integrativa: Método de pesquisa para a incorporação de evidências. *Revista da Escola de Enfermagem da USP*, 50(4), 678–685. <https://doi.org/10.1590/S0080-623420160000500018>
- Meurer, M. I., et al. (2023). Proteção de dados pessoais e desafios na saúde conectada. *Texto & Contexto Enfermagem*, 32, e20220048. <https://doi.org/10.1590/1980-265X-TCE-2022-0048>
- Organização Mundial da Saúde. (2021). *Ethics and governance of artificial intelligence for health*. Geneva, Switzerland: WHO.
- Silva, A. L., et al. (2021). Segurança da informação em saúde digital: Desafios e perspectivas. *Revista Eletrônica de Enfermagem*, 23, e64512. <https://doi.org/10.5216/ree.v23.64512>
- Silva, R. G., & Moreira, T. R. (2022). A ética nos algoritmos em saúde. *Ciência & Saúde Coletiva*, 27(8), 3245–3254. <https://doi.org/10.1590/1413-81232022278.12592022>
- União Europeia. (2016). Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Regulamento Geral sobre a Proteção de Dados (GDPR). *Jornal Oficial da União Europeia*. Retrieved from <https://eur-lex.europa.eu/eli/reg/2016/679/oj>