SEVEN publicações acadêmicas
EM PARCERIA COM: IEMS UNIASSELVI

Segurança da informação em saúde digital no pós-operatório: Riscos, legislação e práticas éticas

Rafael Alves Freires
Cirurgião Dentista, Mestrando em Cirurgia e Pesquisa Experimental
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: dr.rafael.freires22@gmail.com

Leonardo Gomes de Sousa
Enfermeiro, mestrando em Cirurgia e Pesquisa Experimental
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: leonardocantao13@gmail.com

Jackson Roberto Sousa de Oliveira
Fisioterapeuta, mestrando em cirurgia e pesquisa experimental
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: jack.roberto21@gmail.com

Anderson Daniel Viana Pantoja
Enfermeiro, mestrando em cirurgia e pesquisa experimental
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: andersondvpantoja@hotmail.com

Camila Ferreira Alves
Fisioterapeuta, mestranda em cirurgia e pesquisa experimental
E-mail: Camila.ferreiraalves01@gmai.com

Brenda Caroline de Andrade Camelo
Enfermeira, mestranda em cirurgia e pesquisa experimental
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: brendacameloo@hotmail.com

Juliana da Costa Furtado
Enfermeira, mestranda em cirurgia e pesquisa experimental Formação: enfermeira, mestranda
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: enf.julianafurtado@outlook.com

Aracélia Vieira da Silva
Advogada, Mestranda em cirurgia e pesquisa experimental
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: vieira-advocacia2011@hotmail.com Endereço: Marabá-Pará

Wanderson Alexandre da Silva Quinto
Docente, Doutor em psicologia e mestre em engenharia elétrica
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: w.quinto@uepa.br

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.

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

1 INTRODUÇÃO

A crescente digitalização dos serviços de saúde, catalisada pelo avanço das tecnologias da informação e comunicação, tem promovido transformações significativas na forma como o cuidado em saúde é ofertado, especialmente no contexto pós-operatório. Recursos como aplicativos móveis voltados à saúde, plataformas de telemedicina, sistemas de prontuário eletrônico e dispositivos de monitoramento remoto passaram a desempenhar papel central no acompanhamento clínico de pacientes após procedimentos cirúrgicos. Essas ferramentas permitem o envio contínuo de dados fisiológicos, como temperatura corporal, frequência cardíaca e pressão arterial, bem como o registro de sintomas, facilitando uma vigilância clínica mais próxima, mesmo à distância. Além disso, possibilitam uma comunicação mais rápida e eficiente entre pacientes e profissionais da saúde, o que pode favorecer intervenções precoces diante de sinais de complicações. Essa nova lógica de assistência potencializa a continuidade do cuidado, promove maior autonomia ao paciente e contribui para a redução de internações hospitalares desnecessárias.

Entretanto, a integração de fluxos digitais de informação na assistência pós- operatória também impõe desafios consideráveis, especialmente no que se refere à segurança da informação e à proteção da privacidade dos indivíduos. O ambiente digital, ao mesmo tempo em que oferece facilidades operacionais, pode se tornar um espaço vulnerável, exposto a riscos como vazamento de dados sensíveis, acesso não autorizado, uso indevido de informações clínicas e falhas nos sistemas de autenticação. Tais incidentes comprometem não apenas a confidencialidade das informações, mas também a relação de confiança entre pacientes e instituições, podendo gerar danos éticos, legais e psicológicos irreparáveis.

Diante desse cenário, o presente artigo tem como objetivo desenvolver uma análise integrativa e aprofundada sobre a segurança da informação no âmbito da saúde digital direcionada ao cuidado pós-operatório. A investigação concentra-se na identificação e categorização dos principais riscos digitais associados ao uso de tecnologias na fase pós-cirúrgica, bem como na revisão dos marcos regulatórios aplicáveis, com ênfase na Lei Geral de Proteção de Dados Pessoais (LGPD), vigente no Brasil, e no Regulamento Geral sobre a Proteção de Dados (GDPR), em vigor na União Europeia. Além disso, discute-se as implicações éticas decorrentes da adoção dessas tecnologias, tanto para os profissionais da saúde, que devem assegurar condutas pautadas pela confidencialidade e respeito ao consentimento informado, quanto para as instituições, que têm a responsabilidade legal e moral de proteger os dados dos usuários frente às ameaças do ambiente digital. Trata-se, portanto, de uma reflexão que busca articular os aspectos técnicos, jurídicos e éticos relacionados à proteção de dados sensíveis em um contexto de crescente informatização dos serviços de saúde.

2 METODOLOGIA

Trata-se de um estudo de revisão integrativa da literatura, cujo objetivo foi reunir, analisar e sintetizar criticamente produções científicas, documentos legais e diretrizes técnico-normativas relevantes sobre a segurança da informação no contexto da saúde digital aplicada ao cuidado pós-operatório. A coleta de dados foi realizada entre abril e julho de 2025, contemplando publicações disponíveis no período de 2015 a 2025. Para a busca sistematizada, foram utilizadas bases de dados científicas nacionais e internacionais, incluindo PubMed, Scopus, SciELO, LILACS e Google Scholar, bem como repositórios jurídicos especializados, como Jusbrasil e LegisWeb.

Foram empregados os seguintes descritores e termos combinados, em português, inglês e espanhol, de acordo com o vocabulário controlado DeCS/MeSH: “segurança da informação”, “saúde digital”, “pós-operatório”, “bioética”, “LGPD”, “privacidade”, e “proteção de dados em saúde”. A estratégia de busca utilizou operadores booleanos (AND, OR) para maior precisão na recuperação das fontes.

Os critérios de inclusão abrangeram: (i) artigos científicos publicados em periódicos revisados por pares; (ii) documentos normativos e legais com aplicabilidade reconhecida no campo da saúde digital; (iii) textos redigidos em português, inglês ou espanhol; e (iv) publicações que demonstrassem pertinência temática, atualidade e relevância científica comprovada. Foram excluídos estudos duplicados, resumos sem texto completo, opiniões não fundamentadas ou publicações que não abordassem diretamente o recorte temático proposto.

A seleção, extração e análise dos dados foram realizadas de forma independente por dois revisores, seguindo uma abordagem sistemática para garantir a consistência e a qualidade da síntese integrativa.

3 A SAÚDE DIGITAL NO PÓS-OPERATÓRIO

O uso da tecnologia no seguimento pós-operatório tem permitido uma abordagem mais eficaz e centrada no paciente. Dispositivos móveis, aplicativos de monitoramento de sinais vitais, plataformas de teleconsulta e prontuários eletrônicos interoperáveis têm sido utilizados para rastrear recuperações, evitar complicações, garantir adesão medicamentosa e oferecer apoio psicossocial.

Entretanto, esse novo cenário também expõe dados sensíveis a riscos como vazamentos em nós de conexão (por Wi-Fi público, por exemplo), falhas em autenticação, uso de dispositivos pessoais não protegidos (BYOD - Bring Your Own Device), entre outros.

4 RISCOS CIBERNÉTICOS NO CONTEXTO PÓS-OPERATÓRIO

Os principais riscos digitais identificados na literatura incluem:

- Roubo de dados pessoais e de saúde;
- Sequestro de informações por ransomware;
- Manipulação indevida de prontuários;
- Uso de informações sensíveis para fins comerciais ou discriminatórios;
- Falta de consentimento digital adequado.

Casos emblemáticos, como o ciberataque ocorrido em 2021 contra uma das maiores operadoras de planos de saúde no Brasil, evidenciam de forma contundente a vulnerabilidade das estruturas de informação no setor da saúde diante das ameaças cibernéticas. Esses episódios revelam não apenas fragilidades técnicas dos sistemas, mas também a insuficiência de políticas robustas de prevenção, resposta e mitigação. As consequências são severas e imediatas, afetando diretamente a confidencialidade, a integridade e a disponibilidade dos dados sensíveis dos pacientes, além de comprometer a confiança pública nas instituições responsáveis pela gestão do cuidado.

5 LEGISLAÇÃO APLICÁVEL: LGPD E GDPR

A Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) estabelece princípios e diretrizes para o tratamento de dados pessoais no Brasil, incluindo de forma expressa o setor da saúde. Conforme a legislação, dados relativos à saúde são classificados como dados sensíveis, o que implica a adoção de salvaguardas adicionais, como consentimento específico, medidas de segurança mais rigorosas e restrições quanto ao compartilhamento não autorizado. De forma análoga, o Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation – GDPR), em vigor na União Europeia desde 2018, incorpora conceitos fundamentais como consentimento explícito, limitação da finalidade, minimização de dados, e o princípio da responsabilidade proativa (accountability).

Ambas as normativas impõem obrigações claras e detalhadas às instituições de saúde no que se refere ao ciclo completo dos dados digitais — desde a coleta e armazenamento até o compartilhamento e descarte. Tais legislações exigem que os agentes de tratamento adotem medidas técnicas e organizacionais adequadas à natureza dos dados tratados, garantindo não apenas a segurança das informações, mas também a transparência e a proteção dos direitos dos titulares. Em um cenário de crescente digitalização da assistência em saúde, o alinhamento às disposições da LGPD e do GDPR constitui um imperativo ético, legal e operacional.

6 ASPECTOS ÉTICOS DA PROTEÇÃO DA INFORMAÇÃO EM SAÚDE

A bioética aplicada ao contexto da saúde digital convida à reinterpretação crítica dos princípios fundamentais beneficência, não maleficência, autonomia e justiça, diante dos desafios impostos pelas tecnologias emergentes. Em cenários marcados pela coleta, armazenamento e compartilhamento massivo de dados sensíveis, a proteção da privacidade deixa de ser apenas uma obrigação técnica e passa a configurar um direito ético essencial, diretamente vinculado à autonomia do paciente. Garantir essa autonomia implica assegurar um processo de consentimento informado robusto, claro e contextualizado, especialmente em ambientes digitais, onde muitas vezes os riscos são invisíveis ao usuário e as decisões são mediadas por algoritmos. Dessa forma, a ética digital em saúde exige práticas que conciliem inovação com responsabilidade, assegurando que os avanços tecnológicos estejam sempre a serviço da dignidade humana.

As práticas devem considerar:

- Transparência no uso dos dados;
- Limitação de acesso por profissionais;
- Registros de auditoria e rastreabilidade;
- Ética no uso de IA e algoritmos no acompanhamento do pós-operatório.

7 BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO

A proteção efetiva da informação passa por ações técnicas e organizacionais:

- Criptografia de dados em repouso e em trânsito;
- Autenticação de múltiplos fatores (MFA);
- Backups regulares;
- Treinamento de equipes sobre cibersegurança e ética digital;
- Auditorias periódicas e gestão de vulnerabilidades.

8 DISCUSSÃO

A literatura contemporânea evidencia uma tensão permanente entre o avanço das inovações tecnológicas aplicadas à saúde e a necessidade de garantir a proteção ética e legal dos dados sensíveis dos pacientes. Por um lado, os recursos digitais empregados no cuidado pós-operatório, como aplicativos de monitoramento, plataformas de comunicação e sistemas de prontuário eletrônico promovem melhorias significativas na eficiência, na continuidade assistencial e na personalização do tratamento. Por outro lado, a implementação acelerada dessas tecnologias, muitas vezes sem o devido investimento em segurança cibernética e sem a consolidação de uma cultura organizacional voltada à proteção de dados, tem exposto instituições e indivíduos a vulnerabilidades críticas.

Estudos apontam que a fragilidade dos sistemas de informação em saúde, associada à ausência de protocolos robustos de segurança e à carência de treinamentos contínuos para as equipes, amplia os riscos de violações à privacidade, uso indevido de dados e quebra da confidencialidade dos princípios fundamentais da bioética. Em muitas organizações, especialmente no setor público e em serviços com infraestrutura limitada, a proteção dos dados ainda não é tratada como prioridade estratégica, o que compromete a confiança dos usuários e expõe os profissionais a dilemas éticos e legais.

Nesse cenário, a governança da informação em saúde digital assume papel central. Exige-se que as instituições adotem políticas integradas de segurança da informação, pautadas não apenas no cumprimento das exigências legais, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia, mas também nos princípios éticos da beneficência, autonomia, justiça e não maleficência. A adesão a protocolos internacionais de boas práticas em cibersegurança, o fortalecimento do consentimento informado em ambientes digitais e a promoção da educação permanente em ética digital são estratégias fundamentais para mitigar riscos e garantir a integridade do cuidado.

Portanto, a superação desse aparente paradoxo entre inovação e proteção depende do reconhecimento de que a segurança da informação não é um obstáculo à modernização, mas um pilar essencial para sua legitimidade e sustentabilidade. O desafio contemporâneo está em alinhar os avanços tecnológicos com uma governança ética, transparente e centrada no paciente, assegurando que a humanização do cuidado também se expresse na proteção responsável dos dados em ambientes digitais.

9 CONSIDERAÇÕES FINAIS

A segurança da informação no âmbito da saúde digital, especialmente no contexto pós-operatório, deve ser compreendida para além de uma exigência meramente técnica ou legal. Trata-se de um componente essencial de uma prática ética, segura e verdadeiramente centrada no paciente. A integridade e a confidencialidade dos dados sensíveis não apenas sustentam a confiança entre usuários e profissionais da

saúde, mas também representam garantias fundamentais dos princípios bioéticos da autonomia, da beneficência e da justiça.

Proteger os dados dos pacientes é assegurar que suas informações pessoais e clínicas sejam utilizadas de forma transparente, responsável e respeitosa, contribuindo para decisões clínicas mais seguras e relações terapêuticas mais sólidas. No cenário contemporâneo, onde o cuidado digital se torna cada vez mais presente e abrangente, negligenciar a proteção de dados equivale a fragilizar os direitos dos cidadãos e comprometer a legitimidade das tecnologias em saúde.

Nesse sentido, a construção de uma cultura institucional orientada pela ética digital é imperativa. Ela requer o fortalecimento de políticas de governança da informação, investimentos contínuos em cibersegurança, qualificação das equipes multidisciplinares e ampliação do debate público sobre os direitos dos pacientes em ambientes digitais. Conclui-se, portanto, que a humanização do cuidado no século XXI passa, de forma incontornável, pela consolidação de práticas que conciliem inovação tecnológica com responsabilidade ética e compromisso com a proteção da dignidade humana.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, 2018.

UNIÃO EUROPEIA. Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Regulamento Geral sobre a Proteção de Dados (GDPR).

SILVA, A. L. et al. Segurança da informação em saúde digital: desafios e perspectivas. Revista Eletrônica de Enfermagem, 2021.

LOPES, F. C.; RAMOS, M. Bioética e proteção de dados em saúde. Interface, 2020.

DIAS, L. M. et al. Cibersegurança em sistemas de saúde: uma revisão integrativa. Revista Brasileira de Enfermagem, 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo para Agentes de Tratamento de Pequeno Porte. 2021.

SILVA, R. G.; MOREIRA, T. R. A ética nos algoritmos em saúde. Ciência & Saúde Coletiva, 2022.

FERNANDES, P. H. et al. Uso de aplicativos em pós-operatório e segurança da informação. Journal of Health Informatics, 2020.

FERREIRA, J. R.; LUZ, T. C. Riscos digitais em ambientes hospitalares. Informática em Saúde, 2019.

GREENHALGH, T. et al. Digital health and the ethics of care. The Lancet Digital Health, 2021.

KLUGE, E.-H. W. Ethical and legal challenges for health telematics. Studies in Health Technology and Informatics, 2016.

MEURER, M. I. et al. Proteção de dados pessoais e desafios na saúde conectada. Texto & Contexto Enfermagem, 2023.

ORGANIZAÇÃO MUNDIAL DA SAÚDE. Ethics and governance of artificial intelligence for health. Genebra: OMS, 2021.

LUNA, F. Privacy and vulnerability in digital health. Journal of Medical Ethics, 2020.

AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. Diretrizes de segurança da informação para operadoras. 2022.

CONSELHO NACIONAL DE JUSTIÇA. Diretrizes de LGPD no Judiciário. 2023.

MENDES, K. D. S. et al. Revisão integrativa: método de pesquisa para a incorporação de evidências. Revista da Escola de Enfermagem da USP, 2016.

ISO/IEC 27001. Sistemas de gestão de segurança da informação.