Tipo de Trabalho: Trabalho Completo
Seção: Direito em Saúde

PRIVACIDADE E PESQUISA MÉDICA: COMO PROTEGER DADOS DE PACIENTES EM PRONTUÁRIOS ELETRÔNICOS[1]

Nadini Casali Bandeira[2], Luiz Mário Cavalheiro Bortolini[3], Gloria Charão Ferreira[4].

[1] O presente artigo é um desdobramento do tema abordado no projeto de pesquisa de mestrado, submetido ao Programa de Desenvolvimento Regional, na Universidade Regional do Noroeste do Estado do Rio Grande do Sul.

[2] Mestranda bolsista CAPES (PROSUC) – Modalidade I no Programa de Pós-Graduação *Stricto Sensu* em Desenvolvimento Regional pela Universidade Regional do Noroeste do Estado do Rio Grande do Sul – UNIJUÍ. Bacharel em Direito pela Universidade Regional do Noroeste do Estado do Rio Grande do Sul – UNIJUÍ. Advogada. E-mail: nadini.bandeira@sou.unijui.edu.br.
[3] Estudante do Curso de Medicina na Universidade Regional do Noroeste do Estado do Rio Grande do Sul – UNIJUÍ. E-mail: luiz.bortolini@sou.unijui.edu.br.
[4] Profa. Dra. e orientadora na Universidade Regional do Noroeste do Estado do Rio Grande do Sul. Programa de Pós-Graduação *Stricto Sensu* em Desenvolvimento Regional – UNIJUÍ. E-mail: gloria.ferreira@unijui.edu.br.

RESUMO

Introdução: A pesquisa médica com dados de prontuários eletrônicos enfrenta desafios éticos e legais devido à sensibilidade das informações e ao risco de violação da privacidade dos pacientes. **Objetivo**: Analisar estratégias para garantir a privacidade dos dados enquanto viabiliza seu uso para pesquisa médica. **Método**: Realizou-se uma revisão bibliográfica, incluindo artigos científicos das bases PubMed, Scopus e SciELO, além da análise da legislação vigente sobre proteção de dados. **Resultados**: Foram identificadas estratégias como o consentimento do paciente, o cumprimento das normativas legais e das diretrizes dos Comitês de Ética em Pesquisa (CEPs), além do uso de técnicas como anonimização, pseudoanonimização, criptografia, privacidade diferencial e *blockchain*. **Conclusão**: O estudo reforça a necessidade de equilibrar a proteção de dados com o avanço da pesquisa médica, sugerindo a realização de pesquisas empíricas, a colaboração internacional e o desenvolvimento de novas tecnologias para aprimorar a segurança e a eficiência no manejo de dados sensíveis.

INTRODUÇÃO

Ao longo dos anos, o desenvolvimento das redes resultou na crescente complexidade dos aplicativos e na diversificação das tecnologias associadas. No contexto das aplicações médicas, a tecnologia da informação desempenha um papel fundamental na ampliação das funcionalidades clínicas e na otimização do gerenciamento da informação médica (Chen *et al.*, 2021).

Além de aprimorar a capacidade de armazenamento, essas novas tecnologias viabilizam o processamento, a transmissão e a disseminação de dados, possibilitando a troca eletrônica de informações de interesse tanto para os profissionais de saúde quanto para os próprios pacientes.

No entanto, essa digitalização também impacta diretamente a segurança e a privacidade das informações, exigindo a adoção de mecanismos eficazes para a proteção dos dados sensíveis e a garantia do cumprimento das normativas de confidencialidade no contexto médico (Magnagnagno; Luciano; Lüberk, 2021).

Dessa forma, o processamento de dados pessoais em prontuários médicos eletrônicos deve estar em conformidade com os fundamentos jurídicos aplicáveis, garantindo sua legalidade e legitimidade. Para tanto, é necessário o cumprimento de uma série de requisitos, incluindo a obtenção do consentimento expresso do titular dos dados para o acesso e uso das informações, especialmente quando destinadas à realização de pesquisas (Lima *et al.*, 2021).

Um dos debates recorrentes na área diz respeito ao equilíbrio entre a proteção da privacidade das informações de saúde dos indivíduos e os benefícios gerados para a sociedade. Em determinados contextos, ocorre que a exigência do consentimento pode representar um obstáculo à realização de pesquisas, especialmente quando se trata do uso de dados históricos, de indivíduos falecidos, de pacientes com condições que comprometem a cognição ou daqueles que não podem ser localizados (Lima; Ferreto; Buzanello, 2023).

Assim, nesses momentos busca-se reforçar a proteção da privacidade dos dados de cada participante, através de estratégias e mecanismos aplicados para garantir os direitos dos titulares. Em essência, o desafio não consiste em optar entre privacidade e compartilhamento de dados, mas em estabelecer os requisitos essenciais de privacidade, segurança, transparência e confiabilidade que possibilitem um compartilhamento eficiente e responsável de dados na pesquisa médica (Ienca, 2023).

Diante disso, a pergunta problema que conduz este artigo pode ser definida como: **quais estratégias estão sendo implementadas para garantir a privacidade dos pacientes enquanto se facilita o acesso a prontuários eletrônicos para fins de pesquisa médica?**

Destarte, o presente estudo tem como objetivo verificar os mecanismos e práticas adotados pelos sistemas de saúde, tanto no Brasil quanto no cenário internacional, para garantir a proteção dos dados dos pacientes registrados em prontuários eletrônicos e utilizados na pesquisa médica.

METODOLOGIA

A metodologia adotada neste estudo consistiu em uma revisão bibliográfica, fundamentada na leitura e análise de artigos científicos extraídos de bases de dados reconhecidas, tais como PubMed, Scopus e SciELO, além da análise das legislações vigentes que abarcam o tema. Além disso, foram consultadas obras fundamentais para a complementação do embasamento teórico. A seleção dos artigos foi realizada por meio da utilização dos seguintes descritores: “Privacidade dos Pacientes e Prontuários Eletrônicos”, “Consentimento Informado e Pesquisa Médica”, “LGPD e Proteção de Dados em Saúde”, “Anonimização de Dados e Ética na Pesquisa”, “Direitos dos Pacientes e Acesso a Dados de Saúde” e “Comitê de Ética e Consentimento”. Os termos foram empregados de forma individual e combinada, conforme a necessidade da pesquisa. A partir do material coletado, foram selecionados 20 artigos que abordavam a temática com maior profundidade. Após a leitura crítica desses estudos, foram escolhidos aqueles que apresentavam maior relevância para a resposta à pergunta-problema deste artigo.

RESULTADOS E DISCUSSÃO

A condução da pesquisa médica deve ser pautada em princípios éticos que assegurem a proteção dos direitos dos indivíduos. No entanto, a consolidação das diretrizes que orientam as pesquisas contemporâneas resultou de um extenso processo de formulação de normativas e resoluções. Goldim (2002) estabelece que o primeiro alinhamento do Brasil às questões éticas correlacionadas à pesquisa médica ocorreu quando o país aderiu à Declaração de Helsinki, em 1964. Essa declaração foi elaborada pela Associação Médica Mundial e pode ser compreendida como um conjunto de orientações e normas que ressaltam a importância do respeito à dignidade dos participantes da pesquisa, prevalecendo, inclusive, sobre o resultado científico (Lima; Ferreto; Buzanello, 2023).

Nos anos subsequentes, outras resoluções foram desenvolvidas, mas ainda apresentavam lacunas em suas orientações. Dessa forma, após ampla consulta à comunidade científica, profissionais da área da saúde e participantes civis, o Conselho Nacional de Saúde (CNS) elaborou a Resolução 196/1996. Inspirada em legislações internacionais, essa normativa estabeleceu diretrizes fundamentais para a proteção da pessoa humana na condução de pesquisas (Brauner, 2022).

A referida resolução também deu origem à Comissão Nacional de Ética e Pesquisa (CONEP), que se subordina ao Conselho Nacional de Saúde (CNS) e, através da atuação de seus conselhos regionais ou locais CEPs, responsabiliza-se pelas análises éticas em pesquisas com humanos, através da fiscalização de investigação de pesquisa submetidas pelos pesquisadores (Lima; Ferreto; Buzanello, 2023).

Destaca-se que uma das diretrizes fundamentais estabelecidas pelos Comitês de Ética em Pesquisa (CEPs), para a condução de estudos envolvendo seres humanos, é a necessidade do consentimento. Nesse contexto, no âmbito da pesquisa médica, uma das estratégias mais recorrentes para garantir a proteção da privacidade dos participantes é a adoção do Termo de Consentimento Informado. Entretanto, Brauner (2022, p. 13) evidencia que o país ainda apresenta como uma prática recorrente a predominância do "paternalismo médico, o que faz com que o consentimento do paciente ou do voluntário na pesquisa seja, muitas vezes, percebido como uma mera formalidade a ser cumprida".

Nesse sentido, a utilização de dados pessoais de pacientes, obtidos por meio de prontuários médicos, exige a obtenção do consentimento livre, informado e inequívoco do titular. Tal exigência encontra respaldo em um arcabouço jurídico amplo, que abrange legislações e normativas em níveis nacional e internacional, com destaque para a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD), a qual estabelece diretrizes específicas para o tratamento de dados pessoais, incluindo aqueles relacionados à saúde.

O artigo 5º, inciso II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados) classifica os dados relacionados à saúde como dados pessoais sensíveis**,** os quais demandam um nível elevado de proteção durante seu tratamento. Essa exigência decorre da maior vulnerabilidade à qual o titular dessas informações pode estar sujeito, reforçando a necessidade de cautela e segurança no tratamento desses dados.

Destarte, os dados de saúde podem ser definidos como aqueles referentes ao estado físico e mental de um indivíduo, sendo coletados em ambientes clínicos. A responsabilidade pela sua inclusão nos prontuários médicos dos pacientes recai sobre o profissional de saúde, especialmente o médico (Brauner, 2022).

Ressalta-se, portanto, a necessidade de proteger a privacidade desses dados sensíveis. Até a promulgação da Lei Geral de Proteção de Dados, em 2018, outras legislações eram utilizadas

como orientações basilares para a confidencialidade dos dados pessoais e sensíveis, além da exigência do consentimento para utilização destes para fins específicos, tais como a Constituição Federal (1988), o Código Civil (Lei 10.406/2002), o Código de Processo Civil (Lei 13.105/2015), o Código Brasileiro de Defesa do Consumidor (Lei 8.078/1990), o Código Penal (Decreto-Lei 2.848/1940), a Lei de Acesso a à Informação (Lei nº 12527/2011) e pelo Marco Civil da Internet (Lei Federal nº 12965/2014 e Decreto nº 8771/2016) (Lima; Ferreto; Buzanello, 2023).

Além disso, a exigência do consentimento do paciente participante da pesquisa, assim como a necessidade de assegurar a privacidade dos dados contidos nos prontuários eletrônicos, também está prevista em normativas médicas específicas, tais como: Código de Ética Médica (Resolução CFM 2.217/2018), pareceres do Conselho Federal de Medicina (Parecer 8/2005 e 6/2010), Resolução Normativa 21/2002 da Agência Nacional de Saúde Suplementar e as Resoluções 1.605/2000, 1.638/2002, 1.639/2002 e 1.642/2002 do Conselho Federal de Medicina (Lima; Ferreto; Buzanello, 2023).

Evidencia-se, portanto, a relevância do Termo de Consentimento Livre e Esclarecido, cuja elaboração envolve diversas etapas. A Resolução nº 466 de 2012, promulgada pelo Conselho Nacional de Saúde (CNS), em sua seção IV.1, destaca que o pesquisador tem a responsabilidade de fornecer ao participante da pesquisa, ou ao seu representante legal, informações claras e acessíveis sobre os procedimentos e detalhes do estudo. Ademais, esse processo deve considerar a individualidade do participante, a fim de garantir uma comunicação precisa e assegurar que seja concedido um período adequado para a reflexão antes da tomada de decisão quanto à sua participação (Brasil, 2012).

Após dado o consentimento, os agentes envolvidos na pesquisa devem considerar o estabelecido no art. 13 da Lei Geral de Proteção de Dado que prevê que, na execução de estudos em saúde pública, os órgãos de pesquisa poderão acessar bases de dados pessoais, mas que deverão ser tratados exclusivamente no âmbito da instituição responsável, estritamente para a finalidade de pesquisa (Brasil, 2018).

O processamento e o armazenamento dessas informações devem ocorrer em ambientes controlados e seguros, em conformidade com regulamentações específicas de segurança. Ademais, sempre que viável, devem ser implementadas técnicas de anonimização ou

pseudonimização dos dados, assegurando a observância dos princípios éticos e normativos aplicáveis à pesquisa científica (Brasil, 2018).

Por esse viés, os dados utilizados para a realização da pesquisa científica são retirados do prontuário médico do paciente participante. O prontuário médico é um documento destinado ao registro e à preservação das informações relacionadas ao tratamento do paciente, abrangendo os eventos clínicos ocorridos durante a assistência prestada. Além dessa função, o prontuário desempenha um papel fundamental como meio de comunicação entre os profissionais de saúde, possibilitando o compartilhamento de informações essenciais tanto para a condução do tratamento quanto para a realização de pesquisas. Esse registro pode ser mantido em formato físico ou eletrônico (Massad *et al.*, 2003).

Ademais, hospitais públicos e privados, bem como clínicas e unidades de saúde, possuem a obrigação legal de garantir a segurança desses prontuários eletrônicos. Conforme estabelecido pela Resolução nº 7, de 24 de novembro de 2016, do Ministério da Saúde, esses documentos devem conter todas as informações relevantes sobre o paciente (Magnagnagno; Luciano; Lüberk, 2020).

Diante disso, a importância de proteger os dados expostos no prontuário do paciente torna-se ainda maior, em razão que podem vir a ser utilizados para uma análise de dados comparativamente a toda população (Albuquerque Junior; Santos, 2013). Assim, “cada organização deve estabelecer quais políticas serão utilizadas para a proteção desses dados, tendo como base suas necessidades, requisitos legais cultura interna e sistemas informatizados” (Ferreira; Araújo, 2008, p. 34).

É fundamental salientar que o PEC e-SUS APS, utilizado no Sistema de Saúde brasileiro, não foi projetado para interoperar com sistemas externos, seja para a transferência de dados ou para o intercâmbio de informações entre serviços. Diante disso, destaca-se a responsabilidade da administração municipal e das empresas contratadas em garantir a manutenção e a adaptação dos sistemas, assegurando a conformidade com os requisitos de segurança, proteção de dados e interoperabilidade (Celuppi *et al.*, 2024).

Sob esse viés, Magnagnagmo, Luciano e Lüberuk (2020) expõem os resultados de uma pesquisa realizada em dois grandes hospitais brasileiros, cujos participantes era profissionais técnicos de informação, que eram diretamente responsáveis pela adoção de medidas de proteção nesses

locais. Os autores apresentaram, portanto, as ações mais utilizadas, correlacionando-as com os tipos de mecanismos estabelecidos por Guldentops *et al.* (2004).

Guldentops *et al.* (2004) divide os mecanismos em três modalidades. Os primeiros são mecanismos de estrutura, que buscam criar regras e papéis de cada ator dentro de um contexto, o segundo são mecanismos de processo, conceituados pela implementação de sistemas de tomada de decisão e gerenciamentos práticos, no caso, estratégias aplicadas na tecnologia de informação e, por fim, os mecanismos de relacionamento, que seriam a conexão entre o negócio, as ações tomadas e os atores.

Assim, Magnagnagmo, Luciano e Lüberuk (2020) demonstraram que dentro dos hospitais, focos de sua pesquisa, os mecanismos de estrutura mais destacados foram: a existência de uma estrutura física adequada para o gerenciamento do sistema de informação; a necessidade de haver um responsável pela Política de Segurança de Informação; e, a necessidade de proteções internas para a conexão de um novo *hardwere* ou *software* na rede.

Da mesma forma, em relação aos mecanismos de processo, destacaram-se a identificação e autenticação dos usuários; o acesso dos prontuários eletrônicos aos colaboradores da TI, somente com a necessidade legítima; o treinamento constante dos colaboradores; a existência de sanções adequadas para os que violam as políticas de privacidade; utilização do certificado digital nos prontuários eletrônicos e uso de criptografias para o tráfego externo das informações (Magnagnagmo; Luciano; Lüberuk, 2020).

Por fim, acerca dos mecanismos de relacionamento, evidenciaram a criação e a divulgação aos colaboradores de políticas de privacidade; o envio de comunicados constantes aos colaboradores, orientando sobre a proteção da informação e o uso da internet para consulta dos documentos de políticas (Magnagnagmo; Luciano; Lüberuk, 2020)

Assim, denota-se que o sistema de saúde brasileiro opta pelo uso do consentimento e da adequação das pesquisas às normativas legislativas. Entretanto, nem sempre é possível obter esse consentimento, em razão de ser um estudo *post mortem* do paciente ou ser um contexto de pandemia, que dificulta a recolha das autorizações e exige um resultado rápido, como ocorreu nos casos da COVID-19. Para tanto, o presente estudo buscou evidenciar, também, os mecanismos de proteção de dados para pesquisa, utilizados por pesquisadores americanos e europeus.

Segundo Wirth, Meures, Johns e Prasser (2021), uma das alternativas a ser utilizada quando não for possível a obtenção do consentimento é a anonimização. Essa prática consiste na alteração dos dados dos pacientes de forma que eles não possam mais ser identificados.

Para Gadotti, Rocher, Houssiau, Cretu e Montjoye (2024, p. 2), “usamos a anonimização para descrever qualquer processamento de dados pessoais que resultem em informações anônimas, enquanto a “desidentificação” usamos para nos referirmos a um conjunto específico de técnicas de anonimização” (tradução nossa). Os autores também ressaltam que deve ser observado um equilíbrio cuidadoso entre a possibilidade de identificação do titular dos dados e a precisão destes.

Ocorre que a anonimização exige determinados requisitos, de acordo com cada legislação. A GDPR, que é o Regulamento Geral sobre Proteção de Dados, aplicado na Europa, por exemplo, dificulta a sua aplicação, uma vez que a normativa não estabelece os requisitos concretos para sua aplicação e enfrenta interpretações legais diferentes (Wirth; Meures; Johns; Prasser, 2021).

Por outro lado, a Lei Geral de Proteção de Dados (LGPD), em seu artigo 5º, inciso XI, define a anonimização como a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" (Brasil, 2018). No entanto, embora o legislador tenha considerado a necessidade de sua regulamentação, a definição dos meios técnicos e razoáveis para a implementação desse processo permanece genérica, sem especificações detalhadas sobre os métodos a serem adotados.

Diante disso, Wirth, Meures, Johns e Prasser (2021) mencionam que esses desafios podem ser superados pela utilização de infraestruturas de compartilhamentos de dados, que permitem que diferentes locais e base de dados (como hospitais realizando uma pesquisa em conjunto) realizem a análise e o intercâmbio de dados, chegando a um resultado comum, sem que haja a individualização desses dados. Os autores destacam, ainda, que há diversas abordagens para viabilizar esse compartilhamento de informações. Entre elas, ressalta-se o intercâmbio de estatísticas agregadas, no qual os dados são combinados de maneira a fornecer um resultado consolidado. Além disso, destaca-se a aplicação de protocolos criptográficos que possibilitam o processamento conjunto de funções sobre dados privados, garantindo que cada parte envolvida mantenha a confidencialidade de suas respectivas informações de entrada.

Não obstante, Dwork (2008) prevê que embora processados, existem dados que ainda podem se manter identificáveis, como a divulgação de tabelas estatísticas com contagens de células pequenas. Para esses casos, utiliza-se uma técnica inovadora denominada de Privacidade Diferencial que desenvolve uma matemática geral para algoritmos de processamento de dados que torna os dados não identificáveis.

Adicionalmente, destaca-se a prática da pseudonimização, a qual, segundo Gadotti *et al.* (2024), consiste na remoção de identificadores diretos, como nome, endereço e número do seguro social, ou na substituição desses elementos por um pseudônimo gerado aleatoriamente. No entanto, esse método é comumente empregado como etapa inicial do processo de anonimização, uma vez que, isoladamente, não oferece um nível de segurança suficientemente robusto contra possíveis ataques cibernéticos.

Da mesma forma, o art. 13, caput, também prevê a sua utilização para a pesquisa em saúde, conceituando a prática, em seu §4º como: "o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro" (Brasil, 2018).

Por fim, um estudo desenvolvido por Chen *et al.* (2021) evidenciou um outro mecanismo utilizado para proteger os sistemas de informação interna do hospital e a publicação de registros médicos eletrônicos, criado em 2018, que se denomina como K-Ananomity. Segundo os autores supramencionado, esse mecanismo se configura como um sistema de gestão de informações médicas baseado em *Blockchain*, denominado MedBlock, com o objetivo de administrar os dados dos pacientes de forma segura e eficiente. Desse modo, o sistema utiliza um livro-razão distribuído que incorpora um mecanismo avançado de controle de acesso e um modelo robusto de gestão de permissões. Além disso, o MedBlock se destaca por sua capacidade de minimizar o alto consumo de energia e reduzir a sobrecarga na rede, contribuindo para uma infraestrutura mais otimizada e sustentável.

CONCLUSÕES

Deste modo, o presente estudo evidencia as diversas estratégias atualmente empregadas para garantir a privacidade dos pacientes, ao mesmo tempo em que viabiliza o acesso a prontuários eletrônicos para fins de pesquisa médica.

Observa-se que o sistema de saúde brasileiro adota abordagens majoritariamente orientadas à conformidade com legislações e normativas vigentes, como a Lei Geral de Proteção de Dados (LGPD), as diretrizes do Conselho Federal de Medicina (CFM) e da Agência Nacional de Saúde Suplementar (ANS), além da exigência de submissão das pesquisas à fiscalização dos Comitês de Ética em Pesquisa (CEPs).

Adicionalmente, o país prioriza a obtenção do consentimento dos participantes e, no âmbito das instituições de saúde, emprega uma série de mecanismos voltados à proteção de dados, os quais incluem estruturas organizacionais, processos operacionais e estratégias de governança de relacionamentos.

Por fim, este estudo aborda as estratégias aplicadas em cenários nos quais a obtenção do consentimento não é viável, com ênfase nas práticas adotadas nos Estados Unidos e na Europa. Entre essas estratégias, destacam-se a anonimização e a pseudonimização, o desenvolvimento de infraestruturas para compartilhamento de dados - como o intercâmbio de estatísticas agregadas e o uso de protocolos criptográficos-, bem como a implementação de tecnologias inovadoras, a exemplo da Privacidade Diferencial e do *Blockchain*.

Dessa forma, pode-se afirmar que há diversas estratégias disponíveis para assegurar a proteção dos direitos de privacidade e dos dados pessoais dos participantes no contexto da pesquisa médica. Nesse sentido, cabe às instituições de saúde identificar e adotar as abordagens mais adequadas para garantir a segurança e a conformidade com as normativas vigentes.

O estudo apresentado, que analisa estratégias para garantir a privacidade dos dados de prontuários eletrônicos na pesquisa médica, possui algumas limitações que devem ser consideradas. Em primeiro lugar, a metodologia baseada em revisão bibliográfica, embora valiosa para a síntese do conhecimento existente, pode não capturar a complexidade e os desafios práticos enfrentados no uso real dessas estratégias. Assim, a ausência de dados empíricos ou estudos de caso limita a capacidade de generalizar os resultados para diferentes contextos institucionais ou regionais. Soma-se a isso, o fato de que a revisão bibliográfica pode

ser influenciada pelo viés de publicação, em que estudos com resultados positivos ou significativos têm maior probabilidade de serem publicados.

Outra limitação relevante é a complexidade técnica associada à implementação de algumas das estratégias propostas, como criptografia e *blockchain*, pode representar uma barreira para instituições com menor capacitação técnica ou recursos financeiros insuficientes. Isso pode limitar a adoção generalizada dessas soluções, especialmente em contextos em que a priorização de recursos é um desafio.

Para superar as limitações identificadas e avançar no campo da proteção de dados na pesquisa médica, sugere-se que futuros estudos explorem novas abordagens e aprofundem questões ainda não totalmente resolvidas, tais como: Qual é o impacto real da anonimização na qualidade dos dados utilizados para pesquisa?; Quais estratégias de proteção de dados são mais eficazes em países com regulamentações rigorosas?; Como a proteção de dados impacta o tempo e o custo de pesquisas clínicas?; Como a inteligência artificial pode melhorar a anonimização de dados sem comprometer sua utilidade para pesquisa?; Qual é o impacto de programas de capacitação na adoção de práticas éticas de manejo de dados?; Qual é o nível de confiança dos pacientes em relação ao uso de seus dados para pesquisa?; Como a colaboração internacional pode contribuir para a convergência normativa e a adoção de práticas robustas de proteção de dados na pesquisa médica, considerando as diferenças nas legislações e nas capacidades tecnológicas entre países?".

Espera-se que essas perguntas possam orientar pesquisas futuras, contribuindo para o avanço da proteção de dados na pesquisa médica de forma ética, eficiente e globalmente aplicável.

PALAVRAS-CHAVE: consentimento; estratégias; legislações e normativas; proteção de dados.

AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

REFERÊNCIAS

ALBUQUERQUE JUNIOR, Antonio Eduardo; SANTOS, Ernani Marques do. A percepção da importância de Controles de segurança da informação em hospitais públicos brasileiros. **Revista Eletrônica de Comunicação, Informação & Inovação em Saúde**, [S.l.], v. 6, n. 2 p. 2-18, 2013. Disponível em: https://www.reciis.icict.fiocruz.br/index.php/reciis. Acesso em: 19 mar. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015 2018/2018/lei/l13709.htm. Acesso em: 19 mar. 2025.

BRASIL. Conselho Nacional de Saúde. **Resolução nº 466, de 12 de dezembro de 2012.** Disponível em: https://www.gov.br/conselho-nacional-de-saude/pt-br/acesso-a-informacao/legislacao/resolucoes/2012/resolucao-no-466.pdf. Acesso em: 19 mar. 2025.

BRAUNER, Maria Claudia Crespo. Pesquisa biomédica e proteção de dados: experiência brasileira na proteção de direitos dos participantes das pesquisas. *In*: SALARDI, Silvia; SAPAROTI, Michele; ZAGANELLI, Margareth Vetis. **Direitos humanos e tecnologias morais:** uma perspectiva comparada entre Itália e Brasil. Torino: Giapicelli, 2022. Disponível em: https://repositorio.furg.br/handle/123456789/10943. Acesso em: 19 mar. 2025.

CELUPPI, Ianka Cristina; MOHRL, Eduarda Talita Bramorski; FELIBSERTO, Mariano; RODRIGUES, Thiago Serafim; HAMMES, Jades Fernando; CUNHA, Célio Luiz; WAZLAWICK, Raul Sidnei; DALMARCO, Eduardo Monguilhott. Ten years of the Citizen's Electronic Health Record e-SUS Primary Healthcare: in search of an electronic Unified Health System. **Rev. Saúde Publica**, v. 23, n. 58, 2024. Disponível em: scielo.br/j/rsp/a/7jZL8DrBTxtGjDBzCTRBCGH/?format=pdf. Acesso em: 19 mar. 2025.

CHEN, H.-Y.; WU, Z.-Y.; CHEN, T.-L.; HUANG, Y.-M.; LIU, C.-H. Security Privacy and Policy for Cryptographic Based Electronic Medical Information System. **Sensors**, v. 21, p. 713, 2021. Disponível em: https://pmc.ncbi.nlm.nih.gov/articles/PMC7864482/pdf/sensors-21-00713.pdf. Acesso em: 19 mar. 2025.

DWORK, C. Differential privacy: a survey of results. In: AGRAWAL; M.; DU, D.; DUAN, Z.; LI, A.; editors. **Theory and Applications of Models of Computation.** Proceedings of the 5th International Conference on Theory and Applications of Models of Computation. Berlin: Springer; 2008, p. 1–19. Disponível em: https://doi.org/10.1007/978-3-540-79228-4_1. Acesso em: 19 mar. 2025.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Marcio Tadeu. **Políticas de Segurança da Informação** - Guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2008.

GADOTTI, Andrea; ROCHER, Luc; HOSSIAU, Florimond, CRETU, Ana-Maria; MONTJOYE, Yves- Alexandre de. Anonymization: The imperfect science of using data while preserving privacy. **Science Advances**, v. 10, jul., 2024. Disponível em: https://www.science.org/doi/pdf/10.1126/sciadv.adn7053. Acesso em: 19 mar. 2025.

GOLDIM, José Roberto. O consentimento informado numa perspectiva além de autonomia. **Revista AMRIGS**, Porto Alegre, v. 46, n. ¾, jul./dez., p. 109-116, 2002.
GULDENTOPS, E.; VAN-GREMBERGEN, W.; DE HAES, S. Control and governance maturity survey: establishing a reference benchmark and a self-assessment tool. **Information Systems Control Journal**, [S.l.], v. 6, p.32-35, 2004.

IENCA, Marcello. Medical data sharing and privacy: a false dichotomy? **Swiss Med Wkly,** jan. 2023. Disponível em: https://pubmed.ncbi.nlm.nih.gov/36652693/. Acesso em: 20 mar. 2025.

LIMA, Dartel Ferrari de.; FERRETO, Lirane Elize Defante; BUZANELLO, Márcia Rosângela. Consentimento para processamento de dados de pesquisa em prontuários eletrônicos. **Revista biotética,** v. 31, Brasília, 2023. Disponível em: https://www.scielo.br/j/bioet/a/ggqfjXbhQmZXK4VnbdJmQvQ/?format=pdf&lang=pt. Acesso em: 19 mar. 2025.

LIMA D.F.; LIMA, L.A.; CHRISTOFOLETTI, J.F.; MALACARNE, V. Ética y control social en la investigación científica en Brasil. **Rev Colomb Bioét,** v. 16, n.1, 2021. Disponível em: https://pesquisa.bvsalud.org/portal/resource/pt/biblio-1342499. Acesso em: 20 mar. 2025.

MAGNAGNAGNO, Ordilei Antonio; LUCIANO, Edimara Mezzomo; LÜBERK, Rafael Mendes. Como proteger informações do prontuário eletrônico do paciente: propostas de mecanismos. **Ci.Inf.,** Brasília, DF, v. 49, n.2, p. 23-39, maio/ago. 2020. Disponível em: https://encurtador.com.br/ebSth. Acesso em: 19 mar. 2025.

MASSAD, Eduardo; MARIN, Heimar de Fátima; AZEVEDO NETO, Raymundo Soares de. **O Prontuário do Paciente na Assistência, Informação e Conhecimento Médico**. São Paulo: USP, 2003.

WIRTH, F. N.; MEURERS, T.; JOHNS, M.; PRASSER, F. Privacy-preserving data sharing infrastructures for medical research: systematization and comparison. **BMC Med Inform Decis Mak,** v. 21, n. 242, 2021. Disponível em: https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-021-01602-x. Acesso em: 19 mar. 2025.