TRATAMENTO E SEGURANÇA DE DADOS PARA TELEMEDICINA

FRANCHINI, Gianfranco Rafael
GUIDO, Jeferson Eduardo

RESUMO

Impulsionada tanto pelo aumento da demanda por serviços de saúde quanto pelo avanço das tecnologias digitais, a telemedicina tem se expandido significativamente, oferecendo uma abordagem inovadora para o cuidado com os pacientes; entretanto, sua efetividade depende de uma infraestrutura tecnológica adequada e, sobretudo, da garantia da segurança, confidencialidade e integridade das informações dos pacientes. O presente trabalho tem como objetivo analisar e propor práticas seguras para o tratamento de dados sensíveis em telemedicina, visando promover a proteção integral dessas informações e assegurar a conformidade com as regulamentações vigentes, contribuindo, assim, para o fortalecimento e aprimoramento do sistema de saúde brasileiro. Adotando uma abordagem qualitativa e exploratória, a pesquisa envolve a leitura e análise de diferentes fontes, acompanhada de uma revisão minuciosa da documentação e de um estudo detalhado das normas de segurança aplicáveis à telemedicina. Ao identificar problemas significativos, tais como controle de acessos insuficiente, falhas na preservação do anonimato e dificuldades em garantir a integridade dos dados durante o armazenamento e a transmissão, além de riscos decorrentes de erros humanos e da ausência de auditorias, o estudo propõe a implementação de estratégias eficientes, incluindo o uso de dispositivos de segurança de hardware para proteger chaves digitais, o aprimoramento do gerenciamento de acessos e a adoção de novas tecnologias de segurança, ressaltando que a proteção adequada dos dados é fundamental para conquistar a confiança dos pacientes e assegurar a continuidade da telemedicina, garantindo que as inovações tecnológicas estejam sempre vinculadas à privacidade e à segurança das informações de saúde.

PALAVRAS-CHAVE: Health Insurance Portability and Accountability Act (HIPAA), Lei Geral de Proteção de Dados Pessoais (LGPD), telemedicina.

ABSTRACT

Driven by both increased demand for healthcare services and advances in digital technologies, telemedicine has expanded significantly, offering an innovative approach to patient care. However, its effectiveness depends on adequate technological infrastructure and, above all, on ensuring the security, confidentiality, and integrity of patient information. The present study aims to analyze and propose safe practices for the treatment of sensitive data in telemedicine, with a view to promoting the comprehensive protection of this information and ensuring compliance with current regulations, thus contributing to the strengthening and improvement of the Brazilian healthcare system. Adopting a qualitative and exploratory approach, the research involves reading and analyzing different sources, accompanied by a thorough review of the documentation and a detailed study of the security standards applicable to telemedicine. By identifying significant problems, such as insufficient access control, failures in preserving anonymity, and difficulties in ensuring data integrity during storage and transmission, as well as risks arising from human error and the absence of audits, the study proposes the implementation of efficient strategies, including the use of hardware security devices to protect digital keys, improved access management, and the adoption of new security technologies, emphasizing that adequate data protection is essential to gaining patient trust and ensuring the continuity of telemedicine, guaranteeing that technological innovations are always linked to the privacy and security of health information.

KEYWORDS: Health Insurance Portability and Accountability Act (HIPAA), Lei Geral de Proteção de Dados Pessoais (LGPD), telemedicine.

[1] Acadêmico de Sistemas de Informação Gianfranco R. F. E-mail: grfranchini@minha.fag.edu.br

[2] Orientador FAG Jeferson Eduardo Guido. E-mail: jefersonguido@fag.edu.br

1 INTRODUÇÃO

Diante da crescente demanda por serviços de qualidade e das inovações tecnológicas, surge a telemedicina como solução capaz de superar barreiras geográficas e otimizar o atendimento, constituindo um pilar essencial para o bem-estar individual e a coesão social, ocupando posição central na agenda global contemporânea (SCHAEFER, 2024). Contudo, sua efetivação depende de uma infraestrutura tecnológica confiável, que assegure a segurança, confidencialidade e integridade dos dados dos pacientes (KRUSE et al., 2023).

Configurando um ecossistema complexo, o tratamento de dados na telemedicina exige proteção rigorosa das informações, fundamental para garantir a eficiência e a confiança no serviço (COHEN, 2023). No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece diretrizes rigorosas para o manejo dessas informações, alinhando-se a normas internacionais, como a HIPAA (Health Insurance Portability and Accountability Act), que também visam resguardar a privacidade dos dados de saúde (DONEDA, 2023). A convergência dessas legislações é, portanto, essencial para o desenvolvimento de sistemas robustos e confiáveis (ANPD, 2023).

Entretanto, enfrentando desafios significativos como infraestrutura tecnológica insuficiente, falta de interoperabilidade, fragilidades na segurança dos dados e carência de capacitação profissional, a expansão da telemedicina no país requer atenção detalhada. Neste contexto, o presente trabalho tem como objetivo analisar normas e propor práticas mais seguras para o tratamento de dados sensíveis em telemedicina. Para tal, o estudo estrutura-se a partir de uma revisão sistemática da literatura e de uma análise profunda das normas e padrões de segurança, alicerçando a elaboração de propostas práticas que promovam a proteção integral das informações e assegurem a conformidade com as regulamentações vigentes, contribuindo, assim, para a melhoria do sistema de saúde brasileiro.

2 FUNDAMENTAÇÃO TEÓRICA

A telemedicina constitui um paradigma disruptivo no setor da saúde, ao explorar o potencial das tecnologias digitais para viabilizar o acesso a cuidados médicos a distância (World Health Organization, 2020). O sucesso e a sustentabilidade dessa prática a longo prazo dependem, crucialmente, do desenvolvimento e da aplicação de práticas robustas de tratamento de dados, que devem priorizar, acima de tudo, a segurança, a confiabilidade e a estrita privacidade dos dados sensíveis dos pacientes, os quais são permanentemente

transmitidos, armazenados e processados nesse ambiente. Nesse contexto, a gestão eficaz desses dados configura um imperativo para a aceitação e consolidação da telemedicina, conforme enfatizado por Kruse et al. (2023).

Para que essa solidez no tratamento de dados seja efetiva, tornam-se indispensáveis diversos fatores tecnológicos e regulatórios. A complexidade inerente à manipulação de informações de saúde exige compreensão aprofundada dos mecanismos de proteção e das normas vigentes. A garantia da integridade, confidencialidade e disponibilidade dos dados representa um desafio contínuo, que demanda a adoção de padrões e protocolos de segurança rigorosos, como discutido por Anderson (2020) em seus estudos sobre engenharia de segurança.

2.1 O QUE É A TELEMEDICINA?

Viabilizado pela utilização das Tecnologias da Informação e Comunicação (TICs) em serviços médicos à distância, a telemedicina representa um avanço significativo na área da saúde, rompendo barreiras geográficas e permitindo a interação entre pacientes e especialistas, além de possibilitar o acesso a cuidados médicos sem a necessidade da presença física do paciente (Schaefer & Glitz, 2024).

Englobando desde consultas online e acompanhamento remoto de doenças crônicas (WCS Conectologia, 2024) até a emissão de laudos e diagnósticos à distância, processos que envolvem intensa troca de informações entre profissionais especializados, esse campo tem visto na crescente incorporação da Inteligência Artificial um fator determinante para a melhoria do diagnóstico e a otimização dos fluxos de trabalho (Philips, 2025). Entre seus objetivos centrais destacam-se o aumento do acesso à saúde em regiões remotas e a otimização do uso dos recursos disponíveis, proporcionando maior conveniência e eficiência aos usuários (Silva & Piffer, 2025).

Entretanto, a implementação da telemedicina exige atenção rigorosa à segurança e à privacidade dos dados dos pacientes, protegidos tanto pela ética quanto pela qualidade do atendimento. A adoção da Lei Geral de Proteção de Dados (LGPD) e a formalização do consentimento informado configuram desafios centrais, demandando a adequação dos sistemas, o uso de criptografia de ponta a ponta e a implementação de plataformas seguras, a fim de minimizar os riscos de vazamento de informações sensíveis (Cadernos Ibero-americanos de Direito Sanitário, 2025).

Em síntese, a telemedicina está redefinindo a assistência à saúde, com impactos significativos na acessibilidade, eficiência e capacidade de atender às demandas contemporâneas. Impulsionada pela evolução tecnológica, como a implementação do 5G e outras inovações (Saúde Business, 2025), essa modalidade continua a reformular a prestação do cuidado, mantendo a segurança dos dados como prioridade fundamental.

2.2 A importância do tratamento de dados na telemedicina

Gerando um volume massivo de dados sensíveis, que abarcam desde informações clínicas detalhadas até dados de identificação pessoal, a telemedicina, ao transcender barreiras geográficas e temporais, evidencia a necessidade imperativa de práticas robustas de tratamento de dados, as quais constituem a espinha dorsal para a sustentabilidade e a confiança nesse modelo inovador de assistência à saúde. A garantia da confidencialidade, integridade e disponibilidade dessas informações não se limita a uma exigência regulatória, mas configura-se como um pilar ético fundamental, assegurando a privacidade do paciente e fortalecendo a credibilidade dos serviços. Sem a adoção de medidas transparentes e rigorosas no manejo desses dados, a telemedicina corre o risco de suscitar desconfiança por parte de usuários e profissionais, comprometendo sua expansão e aceitação, conforme enfatizam Gostin & Cohen (2022).

Dada a complexidade do ecossistema da telemedicina, que abrange múltiplos pontos de coleta, transmissão e armazenamento de dados, torna-se imprescindível adotar uma abordagem multifacetada para garantir a segurança das informações. Cada interação — seja uma consulta online, o envio de exames ou o registro em um prontuário eletrônico — configura um ponto potencial de vulnerabilidade caso o tratamento de dados não seja rigoroso. A proteção deve estender-se desde a infraestrutura de rede até as aplicações de software e os dispositivos utilizados, assegurando que as informações permaneçam seguras em todo o seu ciclo de vida. A falha em qualquer uma dessas etapas pode ocasionar vazamentos, uso indevido ou manipulação de dados, acarretando sérias consequências legais e éticas, conforme detalha Anderson (2020).

A conformidade com as regulamentações de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e a Health Insurance Portability and Accountability Act (HIPAA) nos Estados Unidos, constitui um aspecto inegociável no tratamento de dados na telemedicina. Tais legislações impõem diretrizes estritas sobre a coleta, o armazenamento, o processamento e o compartilhamento de dados de saúde, exigindo que as organizações

implementem salvaguardas técnicas e administrativas robustas. A não observância dessas normas pode acarretar multas substanciais e danos irreparáveis à reputação, reforçando a necessidade de um compromisso contínuo com as melhores práticas de governança de dados, conforme enfatizado pela ANPD (2022) em seus guias orientativos.

Além de atender às exigências legais, torna-se fundamental, para um tratamento de dados eficaz, a adoção de tecnologias avançadas de segurança. A proteção criptográfica mostra-se essencial para resguardar a confidencialidade das informações, tornando-as inacessíveis a partes não autorizadas, tanto durante a comunicação quanto no armazenamento. Mecanismos de autenticação forte, como a autenticação multifator, aliados a controles de acesso rigorosos, garantem que apenas profissionais autorizados tenham acesso aos dados dos pacientes. A implementação de Módulos de Segurança de Hardware (HSMs) para a gestão de chaves acrescenta uma camada adicional de proteção, elevando significativamente o nível de segurança do tratamento de dados. Tais práticas encontram respaldo nas diretrizes para a construção de sistemas distribuídos seguros de Anderson (2020) e reforçam a necessidade de infraestruturas robustas para a saúde digital, conforme enfatizam Gostin & Cohen (2023).

Consequentemente, o desenvolvimento e a interoperabilidade plena dos EHRs revelam-se absolutamente cruciais para a modernização do setor de saúde, promovendo não apenas a melhoria da qualidade do atendimento, mas também a eficiência máxima do sistema. Esses prontuários, ao tornarem os processos e a interação entre as equipes fluídos e altamente coordenados, asseguram simultaneamente uma segurança reforçada dos dados, proporcionando uma assistência verdadeiramente integrada e centrada no paciente, apoiada pelas mais avançadas tecnologias da saúde digital. A relevância dos EHRs para a segurança do paciente e a eficiência operacional é amplamente reconhecida na literatura, como evidenciam Hillestad et al. (2021) em suas análises sobre o valor incomensurável da informatização na saúde.

2.3 electronic health records (Prontuários Eletrônicos de Saúde)

Ao constituírem sistemas digitais essenciais e estrategicamente indispensáveis para a gestão de dados médicos, os Prontuários Eletrônicos de Saúde (Electronic Health Records – EHRs) preservam o histórico completo dos pacientes de forma padronizada, segura e estruturada, consolidando-se como um pilar central inquestionável na telemedicina e na proteção de informações sensíveis. Ao assegurar a integridade, a confidencialidade e a acessibilidade das informações clínicas, os EHRs promovem não apenas eficiência máxima e

incomparável no fluxo de trabalho, mas também segurança robusta e sem precedentes no cuidado prestado, conforme destacado por Blumenthal (2022) em seu estudo sobre o papel transformador e inovador desses sistemas.

Por meio da utilização desses prontuários, o acesso aos dados pelos profissionais de saúde torna-se não apenas ágil, mas extraordinariamente confiável, facilitando a tomada de decisões clínicas e contribuindo de maneira significativa para a melhoria contínua da qualidade do atendimento, corroborando simultaneamente as observações de Bates et al. (2023) sobre os benefícios incontestáveis dos sistemas de informação em saúde.

A interoperabilidade e a integração eficaz dos EHRs entre diferentes plataformas e serviços de saúde revelam-se absolutamente indispensáveis para assegurar o fluxo contínuo e ininterrupto das informações, elemento vital para o funcionamento eficiente da telemedicina. Hersh (2021) destacou a interoperabilidade como um desafio central e incontornável, constituindo uma necessidade absoluta para a plena e máxima efetivação dos benefícios dos EHRs. Por meio dessa funcionalidade, os profissionais de saúde passam a acessar os dados apropriados com velocidade e precisão quase instantâneas, promovendo a coordenação do cuidado e elevando de maneira exponencial a segurança do paciente. O investimento em padrões abertos e em tecnologias avançadas de integração é, portanto, crucial para superar os persistentes desafios de compatibilidade e garantir uma visão integral e verdadeiramente holística da saúde do paciente, preocupação constantemente ressaltada por pesquisadores como Mandl & Kohane (2022).

Dessa forma, o desenvolvimento e a plena interoperabilidade dos EHRs revelam-se absolutamente essenciais para a modernização do setor de saúde, promovendo não apenas a melhoria significativa da qualidade do atendimento, mas também a eficiência máxima do sistema. Esses prontuários, ao tornarem os processos e a interação entre as equipes mais fluídos, coordenados e harmoniosos, asseguram simultaneamente uma segurança reforçada dos dados, proporcionando uma assistência verdadeiramente integrada e centrada no paciente, apoiada pelas mais avançadas tecnologias da saúde digital. A relevância dos EHRs para a segurança do paciente e para a eficiência operacional é amplamente reconhecida na literatura, como demonstram Hillestad et al. (2023) em suas análises sobre o valor incomensurável da informatização na saúde.

2.4 principais vulnerabilidades encontradas em sistemas de telemedicina

Os sistemas de telemedicina, ao lidar com informações de saúde altamente sensíveis, enfrentam vulnerabilidades críticas diretamente ligadas ao tratamento dos dados dos pacientes. Uma das falhas mais significativas reside na gestão inadequada de acessos e permissões, que permite que dados confidenciais sejam acessados por indivíduos não autorizados. Isso inclui a concessão de privilégios excessivos, a falta de revisão periódica de permissões e a ausência de segregação de funções, onde um único usuário pode ter acesso a múltiplas etapas do tratamento de dados. Tais deficiências comprometem a confidencialidade e a integridade das informações, facilitando o vazamento ou a manipulação indevida, conforme destacado por KRUSE et al. (2023) em suas análises sobre segurança em saúde digital.

Outra vulnerabilidade crucial no tratamento de dados é a falha na anonimização e pseudo-minimização eficaz das informações. Embora a telemedicina exija o uso de dados identificáveis para o cuidado direto, para fins de pesquisa, análise ou desenvolvimento de sistemas, a capacidade de desidentificar dados é fundamental. Quando os processos de anonimização são falhos ou inexistentes, dados que deveriam ser não identificáveis podem ser associados a indivíduos, violando a privacidade. A ausência de técnicas robustas para proteger a identidade do paciente em cenários onde a identificação não é estritamente necessária representa um risco significativo para a privacidade dos dados tratados, um desafio reconhecido por HIMSS (2023).

Complementando essas vulnerabilidades técnicas, a integridade dos dados durante o armazenamento e a transmissão constitui outro ponto crítico. Vulnerabilidades em bancos de dados, como injeção de SQL ou configurações de segurança padrão, podem permitir que atacantes alterem ou excluam registros de pacientes, comprometendo a precisão das informações de saúde. Similarmente, durante a transmissão, a ausência de mecanismos de proteção adequados pode expor os dados a interceptações e modificações. Garantir que os dados permaneçam inalterados e confiáveis desde a sua coleta até o uso final é um aspecto fundamental do tratamento seguro, e falhas nesse processo podem ter consequências clínicas graves, como apontado por ROMAN et al. (2024).

Além das vulnerabilidades técnicas, é necessário considerar o fator humano como uma fonte significativa de risco. A falta de treinamento específico sobre as políticas de tratamento de dados e as melhores práticas de privacidade para profissionais de saúde e administrativos pode levar a erros operacionais. Isso inclui o compartilhamento acidental de dados sensíveis

por e-mail não seguro, o acesso a informações de pacientes sem necessidade clínica ou o descarte inadequado de registros físicos ou digitais.

Ademais, a engenharia social representa uma ameaça complementar, explorando a confiança humana para obter acesso a dados. Em sistemas de telemedicina, ataques de phishing direcionados a profissionais de saúde para obtenção de credenciais, pretexting para coletar informações de pacientes, ou o uso de iscas digitais para instalar malwares em dispositivos de trabalho são riscos constantes, conforme ressaltado pelo PONEMON INSTITUTE (2023) e reforçado por CYBERSECURITY TRENDS (2024). A complexidade e a sensibilidade dos dados de saúde tornam os sistemas de telemedicina alvos particularmente atraentes, exigindo vigilância e treinamento contínuos para mitigar os riscos (HEALTHCARE IT NEWS, 2025).

Por fim, a ausência de auditorias e monitoramento contínuo constitui uma vulnerabilidade crítica que integra as dimensões técnica e humana. Sem um registro detalhado de quem acessou, modificou ou transmitiu dados, e sem a capacidade de detectar atividades suspeitas em tempo real, as organizações ficam cegas para possíveis violações. A falta de logs de auditoria completos e a ineficácia na análise desses logs impedem a identificação rápida de incidentes e a resposta adequada, prolongando o tempo de exposição e aumentando o dano potencial. A vigilância constante sobre os processos de tratamento de dados é essencial para a detecção e mitigação proativa de riscos, sendo um ponto crucial para a resiliência cibernética, conforme discutido por CISA (2023).

2.5 hardwares security modules

Dispositivos físicos especializados, os Módulos de Segurança de Hardware (HSMs) surgem como guardiões incansáveis da segurança digital, concebidos para gerar, armazenar e proteger chaves criptográficas — pilares essenciais para o tratamento seguro de dados. Em sua função primordial, isolam e resguardam as chaves mestras de cifragem contra acessos não autorizados, garantindo que os elementos mais críticos para a proteção das informações permaneçam em um ambiente altamente seguro e controlado. Essa camada adicional de proteção é indispensável em sistemas que manipulam dados sensíveis, como os da saúde digital, onde a confidencialidade e a integridade das informações dos pacientes são vitais. Ademais, a robustez desses dispositivos é amplamente reconhecida, resistindo tanto a ataques físicos quanto a tentativas lógicas de violação, assegurando a inviolabilidade das chaves de forma praticamente inquebrável.

A utilização de HSMs reforça significativamente a segurança das operações criptográficas, prevenindo que as chaves sejam comprometidas e, consequentemente, protegendo integralmente os dados a elas associados. Essa tecnologia fortalece a confiabilidade dos processos de autenticação, assinatura digital e criptografia, garantindo a integridade e a confidencialidade das informações em todas as etapas de seu tratamento. Os HSMs funcionam como uma verdadeira âncora de confiança para todo o ecossistema de segurança digital, assegurando que operações críticas, como a criação de identidades digitais e a proteção de registros sensíveis, ocorram em um ambiente praticamente imune a adulterações. Anderson (2020) destaca a relevância desses módulos na construção de sistemas distribuídos seguros, reforçando sua posição como elemento central na arquitetura da saúde digital.

A implementação de HSMs configura-se como prática indispensável para infraestruturas de telemedicina e Prontuários Eletrônicos de Saúde (EHRs), onde a proteção dos dados é estratégica. Esses dispositivos garantem que as chaves criptográficas permaneçam em um ambiente físico seguro, protegendo-as contra ciberataques e acessos indevidos, ao mesmo tempo em que favorecem a conformidade com elevados padrões de segurança. Eles desempenham papel crucial na gestão segura do ciclo de vida das chaves, desde a criação até a destruição, minimizando riscos e assegurando que apenas entidades autorizadas possam acessar ou processar dados sensíveis. Gostin & Cohen (2023) enfatizam a importância de infraestruturas robustas e confiáveis para a saúde digital.

No contexto do tratamento de dados em telemedicina, a proteção das chaves criptográficas é essencial para assegurar a integridade e a confidencialidade das informações dos pacientes. Por exemplo, a proteção de chaves usadas para criptografar dados em repouso ou autenticar o acesso de profissionais de saúde é determinante. Mesmo quando médicos utilizam dispositivos individuais criptografados, como pendrives para acessar plataformas de telemedicina — por exemplo, a Plataforma Docway —, a segurança das chaves no sistema central pode ser reforçada pelos HSMs. Assim, mesmo na eventualidade de comprometimento de um dispositivo de acesso individual, a chave mestra que protege grandes volumes de dados permanece isolada e inviolável, garantindo a integridade e a confiabilidade do sistema como um todo.

Portanto, a implementação de HSMs constitui um componente estratégico e fundamental para a segurança de dados na telemedicina, indo além da mera conformidade regulatória. Esses dispositivos não apenas reforçam a proteção contra ameaças externas, mas

também possibilitam o atendimento a exigências rigorosas, fornecendo controle auditável e robusto sobre as chaves criptográficas. Ao centralizar e resguardar as chaves, tanto física quanto logicamente, os HSMs elevam substancialmente o nível de confiança no tratamento de informações sensíveis, configurando-se como investimento essencial para a resiliência e a conformidade dos sistemas de saúde digital, em consonância com as diretrizes da World Health Organization (2021).

2.6 LGPD (Lei Geral de Proteção de Dados Pessoais)

Guardião incontestável da privacidade no Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, estabelece um marco regulatório robusto para o tratamento de dados pessoais, erguendo-se como verdadeiro baluarte dos princípios de Confidencialidade, Integridade, Disponibilidade e Autenticidade (CIDA). A confidencialidade garante que as informações permaneçam acessíveis apenas a pessoas, entidades ou processos autorizados, prevenindo qualquer acesso indevido ou vazamento de dados sensíveis (SANTOS, 2024). No contexto da telemedicina, isso implica que os dados de saúde dos pacientes devem ser protegidos de forma intransigente, ficando disponíveis apenas para profissionais e sistemas devidamente credenciados para o cuidado.

Quanto à integridade, ela assegura que os dados sejam precisos, completos e imutáveis diante de modificações não autorizadas, sejam estas intencionais ou acidentais. Em ambientes de telemedicina, a integridade assume caráter vital, pois qualquer alteração indevida em prontuários eletrônicos, resultados de exames ou planos de tratamento pode gerar diagnósticos equivocados e decisões clínicas inadequadas. A LGPD exige, portanto, que os agentes de tratamento implementem medidas técnicas e administrativas capazes de preservar a exatidão e confiabilidade das informações ao longo de todo o seu ciclo de vida, desde a coleta até o descarte (SANTOS, 2024).

Garantir a disponibilidade significa assegurar que as informações e os sistemas que as processam estejam sempre acessíveis e plenamente utilizáveis por pessoas ou entidades autorizadas. No ambiente da telemedicina, a ausência ou interrupção desses dados pode gerar consequências potencialmente catastróficas, bloqueando atendimentos emergenciais, dificultando o acompanhamento de pacientes crônicos e limitando o acesso a históricos médicos essenciais (SANTOS,2024).

A Autenticidade, por sua vez, consiste em comprovar a origem e a autoria dos dados, além de assegurar que todas as ações realizadas sobre eles possam ser rastreadas e auditadas

com precisão. Nos sistemas de telemedicina, essa garantia é frequentemente implementada por meio de mecanismos de controle rigorosos, entre os quais se destacam as Credenciais de Login — nomes de usuário e senhas, muitas vezes exigindo complexidade elevada e trocas periódicas (SANTOS, 2024).

Certificados Digitais: Emissão de certificados digitais para profissionais de saúde garante a identidade inequívoca e a validade das ações e assinaturas eletrônicas, conferindo ao sistema um nível de confiança quase absoluto (LIMA, 2024).

Autenticação de Dois Fatores (2FA) ou Multifator (MFA): Acrescentar uma camada adicional de verificação — como código enviado por SMS, token de aplicativo ou biometria — além da senha, eleva exponencialmente a segurança dos acessos e dificulta qualquer tentativa de invasão (CYBERSECURITY TRENDS, 2024).

A LGPD, ao exigir a adoção de medidas de segurança, impõe que as organizações assegurem a continuidade dos serviços e o acesso ininterrupto às informações, mesmo diante de falhas de sistema ou ataques cibernéticos, através da implementação de planos de contingência e estratégias de recuperação de dados (ANPD, 2023).

Para cumprir rigorosamente os princípios de Confidencialidade, Integridade, Disponibilidade e Autenticidade (CIDA) sob a LGPD, as organizações de telemedicina devem adotar uma série de medidas técnicas e organizacionais. Entre elas destacam-se a gestão criteriosa de acessos, a criptografia de informações em repouso e em trânsito, a realização de backups periódicos e a implementação de sistemas contínuos de monitoramento. A LGPD também reforça a necessidade de uma governança de dados sólida e da conscientização permanente dos colaboradores. Cumprir esses princípios não apenas atende a requisitos legais, mas configura um imperativo ético, protegendo os direitos fundamentais de privacidade e autodeterminação informativa dos titulares de dados (DONEDA, 2023).

Em síntese, a LGPD não se limita a impor a proteção das informações pessoais; ela estabelece que essa salvaguarda seja firmemente alicerçada nos princípios de confidencialidade, integridade e disponibilidade. No âmbito da telemedicina, isso implica a necessidade de um tratamento de dados que vá muito além da simples conformidade legal, sendo tecnicamente robusto e capaz de assegurar a confiança plena dos pacientes. A conformidade com a LGPD, portanto, exige uma abordagem verdadeiramente holística, que integre de forma contínua e inquebrantável esses três pilares da segurança da informação em todas as operações de tratamento de dados de saúde.

2.7 Health Insurance Portability and Accountability Act

Nos Estados Unidos, a HIPAA (Health Insurance Portability and Accountability Act), promulgada em 1996 (U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, 1996), estabelece padrões nacionais extremamente rigorosos para a proteção das informações de saúde. Reconhecida como a verdadeira espinha dorsal da privacidade médica norte-americana, a HIPAA assegura que dados sensíveis sejam tratados com cuidado absoluto, preservando sua confidencialidade e segurança de maneira praticamente inviolável.

A conformidade com a HIPAA é mandatória para todos os sistemas de telemedicina que operem ou manipulem informações de pacientes em território americano. Seu foco central combina a portabilidade do seguro de saúde com a responsabilidade plena quanto à privacidade, exigindo que as entidades abrangidas implementem salvaguardas administrativas, físicas e técnicas de alto nível. Entre essas medidas, destacam-se a aplicação de criptografia avançada e o controle rigoroso de acessos, garantindo que os dados permaneçam protegidos contra qualquer ameaça, invasão ou violação (Smith & Johnson, 2023).

Embora ambas as legislações compartilhem o objetivo inegociável de proteger dados de saúde, elas se distinguem por abordagens que refletem diferentes filosofias de governança da informação. A HIPAA ergue-se como uma lei setorial rigorosa, dedicada exclusivamente ao setor de saúde norte-americano, traçando normas minuciosas sobre o uso e a divulgação das “Informações de Saúde Protegidas” (PHI), funcionando quase como um manual detalhado de conduta que deixa pouca margem para dúvidas. Em contrapartida, a LGPD apresenta-se como uma legislação de alcance universal, impondo seus princípios a todos os setores que tratam dados pessoais no Brasil e elevando os dados de saúde à categoria de “dado pessoal sensível” — um bem de valor incomensurável, cuja proteção exige rigor máximo e intransigente.

Enquanto a HIPAA oferece um caminho prescritivo e relativamente linear para a conformidade, guiando as organizações passo a passo, a LGPD desafia os agentes de tratamento a construir e justificar, com precisão quase cirúrgica, a robustez das medidas de proteção adotadas. Sob a LGPD, cada decisão sobre segurança não é apenas recomendável, mas uma responsabilidade colossal, cuja falha pode comprometer a confiança pública e a integridade de toda a infraestrutura de dados. Dessa forma, enquanto a HIPAA delimita

fronteiras objetivas, a LGPD exige vigilância contínua e governança proativa, elevando a proteção de dados a um verdadeiro imperativo ético e estratégico para o setor de saúde.

2.8 Estatísticas e Custos de Violações de Dados na Saúde

O setor de saúde permanece como um alvo privilegiado para ataques cibernéticos, com o número de violações de dados e de indivíduos afetados mantendo-se alarmantemente elevado, conforme indicam as estatísticas mais recentes do HIPAA Journal. Tais violações não comprometem apenas informações pessoais e médicas sensíveis de milhões de indivíduos, mas também impõem custos financeiros e danos reputacionais de proporções significativas às organizações.

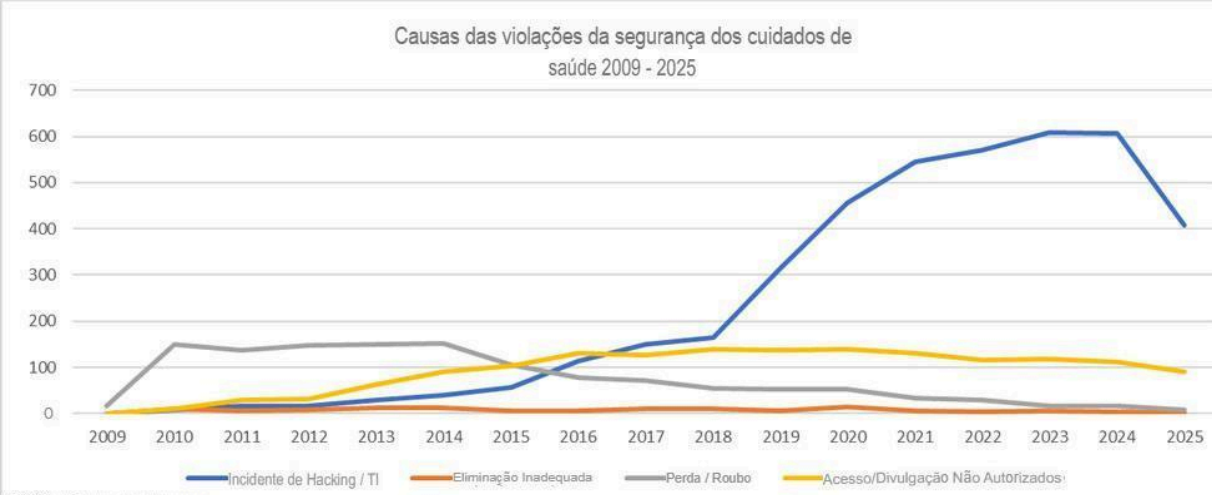
Dados recentes apontam uma tendência consistente de crescimento das violações de dados na última década. Essa escalada é claramente evidenciada no Gráfico 1, que demonstra o aumento contínuo do número de indivíduos afetados ano após ano, com picos que impressionam pela magnitude do risco. O destaque vai para o acentuado aumento observado em 2024, sugerindo a ocorrência de eventos de grande magnitude, como ataques coordenados a redes hospitalares de larga escala ou a violação de provedores de seguros com milhões de clientes. Tais ocorrências extremas expõem de forma dramática a vulnerabilidade sistêmica do setor, reforçando a urgência da implementação de estratégias de defesa robustas e resilientes.

Gráfico 1 – Indivíduos afetados por violações de segurança na saúde (2009-2025)

Fonte: The HIPAA Journal (2025).

O Gráfico 2 detalha essa realidade, mostrando como os incidentes de hacking (linha azul) se tornaram a causa predominante de violações, superando outras categorias como acesso não autorizado, perda ou roubo.

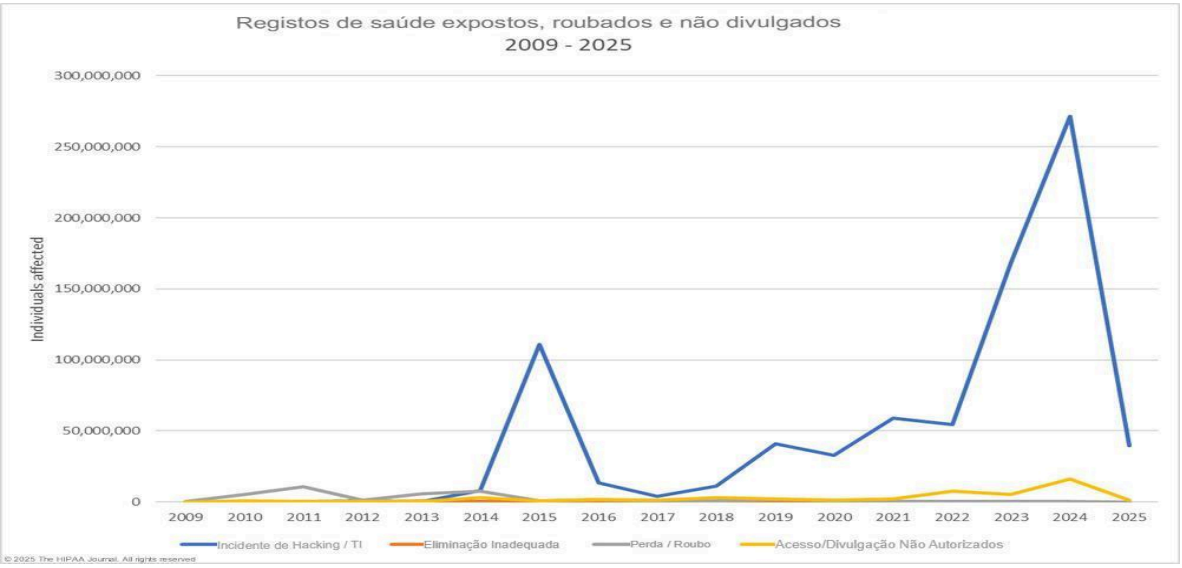
Gráfico 2 – Causas das violações de segurança na saúde (2009-2025)



Fonte: The HIPAA Journal (2025)

Com base no Gráfico 3, o texto aponta que Incidentes de Hacking/TI (linha azul) são a maior ameaça aos registros de saúde, comprometendo o maior número de pacientes (com picos dramáticos em 2015 e 2024) e revelando uma vulnerabilidade sistêmica,em contrapartida, Acessos Não Autorizados (linha amarela), embora recorrentes, expõem um volume muito menor de dados, destacando a importância do fator humano na segurança.Por fim, o texto ressalta que as consequências dessas violações são enormes, indo além do financeiro e impactando severamente a confiança pública e a integridade do sistema de saúde.

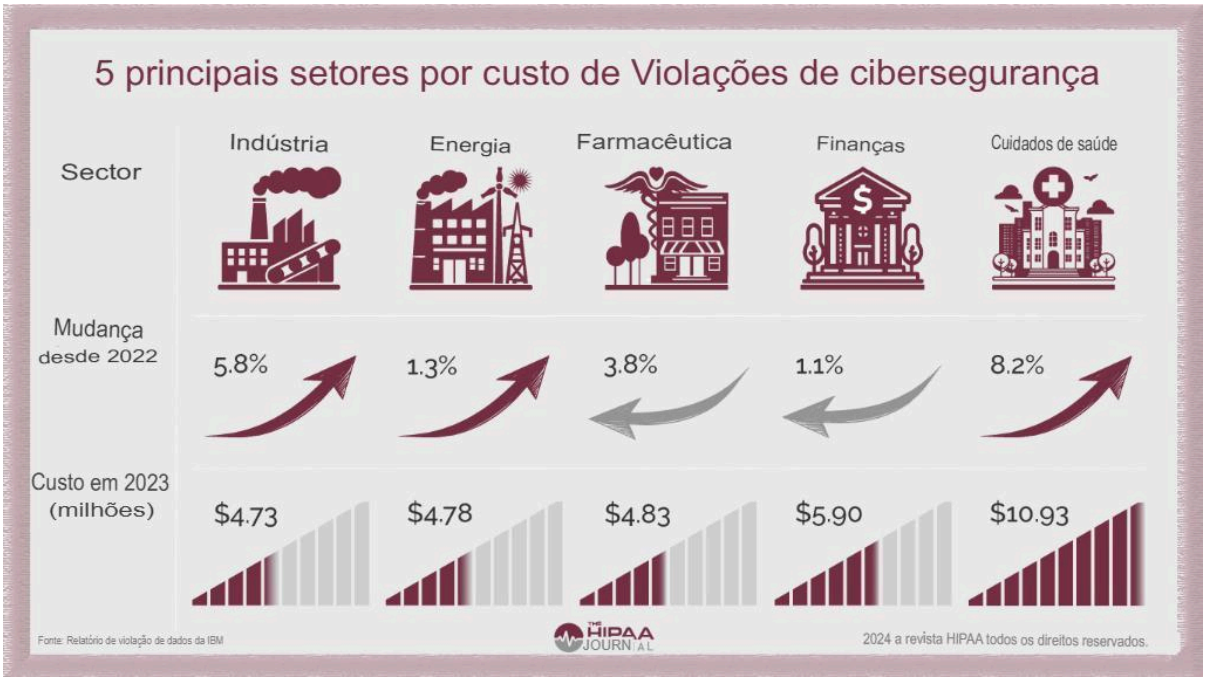
Gráfico 3 – Registros de Saúde Expostos, Roubados e Divulgados sem Permissão (2009-2025)



Fonte: The HIPAA Journal (2025)

Conforme evidenciado no Gráfico 4, a indústria da saúde mantém-se como o setor que arca com os custos mais elevados decorrentes de violações de dados, atingindo a impressionante cifra de US$10,93 milhões em 2023 — um aumento de 8,2% em relação a 2022. O custo médio por registro violado impõe um fardo financeiro considerável, englobando despesas com notificação das violações, serviços de monitoramento de crédito para os indivíduos afetados, multas regulatórias e honorários advocatícios. Tais cifras não apenas refletem perdas econômicas, mas também ressaltam o impacto profundo sobre a confiança dos pacientes, a reputação das instituições e a resiliência de todo o sistema de saúde.

Gráfico 4 – Os 5 setores com maior custo por violações de cibersegurança.



Fonte: The HIPAA Journal (2025)

3 METODOLOGIA

3.1 CARACTERIZAÇÃO GERAL DO MÉTODO

A pesquisa desenvolvida neste trabalho é de natureza bibliográfica, qualitativa e exploratória, com o objetivo de investigar o tratamento de dados aplicado à telemedicina, enfatizando a privacidade e a segurança das informações dos pacientes. Esse levantamento bibliográfico integra duas abordagens metodológicas, permitindo uma compreensão profunda e abrangente do tema. A escolha desse método justifica-se pela complexidade e sensibilidade dos dados de saúde, que exigem uma análise criteriosa das práticas existentes e das regulamentações vigentes.

Para conferir maior rigor metodológico ao estudo, a coleta de fontes foi realizada em bases de dados acadêmicas e científicas de reconhecida relevância, como SciELO, IEEE Xplore, PubMed e Google Scholar. Foram empregados termos de busca e palavras-chave como “Health Insurance Portability and Accountability Act (HIPAA)”, “Lei Geral de Proteção de Dados Pessoais (LGPD)”, “telemedicina”. Priorizou-se a seleção de artigos científicos, livros, relatórios técnicos e guias de boas práticas, majoritariamente publicados entre 2020 e 2025, assegurando a atualidade e pertinência das informações que fundamentam a análise teórica e os desdobramentos subsequentes.

A abordagem bibliográfica possibilita a revisão sistemática do conhecimento previamente consolidado, oferecendo uma base sólida para as análises propostas.

A vertente qualitativa da pesquisa concentra-se nos resultados, buscando compreender de forma aprofundada os temas tratados. Não se limita a dados quantitativos, mas interpreta as razões subjacentes à escolha de determinadas abordagens no tratamento de dados, examinando as nuances das normas e os desafios impostos pela segurança da informação na telemedicina. Trata-se de uma análise interpretativa que enfatiza significados, conceitos e perspectivas relacionadas aos dados em estudo, permitindo identificar padrões, tendências e insights que poderiam passar despercebidos em análises meramente quantitativas.

A pesquisa exploratória é empregada quando o tema investigado é pouco conhecido ou insuficientemente estudado, com o objetivo de proporcionar uma compreensão inicial e identificar questões que demandam aprofundamento. Nesse contexto, ela se mostra essencial para o mapeamento das diferentes abordagens de tratamento de dados utilizadas na telemedicina, das normas vigentes e das tecnologias voltadas à segurança da informação. O enfoque está em reunir e analisar informações sobre um campo complexo e estratégico — a

segurança de dados em telemedicina — que se encontra em constante evolução, exigindo um entendimento abrangente para a formulação de boas práticas e recomendações eficazes.

Objetivos e Abrangência da Pesquisa

Um dos eixos centrais da pesquisa é a conformidade com normas de privacidade e segurança de dados. O estudo buscou avaliar legislações e regulamentações que regem a proteção da privacidade e da segurança das informações dos pacientes, garantindo que as soluções analisadas estejam alinhadas aos requisitos legais e éticos. Tal alinhamento é fundamental para promover a confiança no uso da tecnologia em ambientes de saúde. Em especial, a pesquisa dedica atenção ao Capítulo VII da Lei Geral de Proteção de Dados (LGPD), que aborda especificamente a segurança e as boas práticas no tratamento de dados pessoais, estabelecendo as bases para a proteção de dados sensíveis e reforçando a importância da governança e da responsabilidade no manejo dessas informações.

Revisão e Análise da Literatura e das Normas: A pesquisa apoia-se em uma revisão abrangente da literatura existente sobre o tema, complementada por uma análise minuciosa das normas e regulamentações de segurança aplicáveis ao setor da saúde digital, garantindo uma compreensão sólida e contextualizada do cenário atual.

Ênfase na Integridade, Confidencialidade e Disponibilidade: O estudo busca identificar e propor práticas e tecnologias capazes de assegurar que as informações em telemedicina permaneçam íntegras — precisas, completas e imunes a alterações não autorizadas; confidenciais — acessíveis exclusivamente a usuários devidamente autorizados; e disponíveis — prontamente acessíveis sempre que e onde forem necessárias, reforçando a confiança no uso seguro das plataformas digitais de saúde.

Relevância da Sensibilidade e da Importância: A pesquisa reconhece o caráter crítico e altamente sensível dos dados de saúde, cujo manejo inadequado poderia gerar consequências significativas. Esse contexto justifica a necessidade de um estudo aprofundado e da proposição de soluções robustas, capazes de garantir a proteção ética e a gestão exemplar dessas informações vitais.

Justificativa: A escolha desta metodologia decorre diretamente da natureza complexa do problema de pesquisa, que exige uma compreensão aprofundada das nuances envolvidas no tratamento de dados em telemedicina. Ao combinar abordagens qualitativa e exploratória com uma revisão bibliográfica robusta, é possível não apenas identificar lacunas existentes no conhecimento, mas também propor soluções e diretrizes simultaneamente relevantes, viáveis e contextualizadas. A incorporação do Capítulo VII da LGPD fortalece o compromisso com a

conformidade legal, enquanto a ênfase nos princípios de Confidencialidade, Integridade, Disponibilidade e Autenticidade (CIDA) assegura que os fundamentos essenciais da segurança da informação sejam tratados de forma abrangente. Dessa maneira, a metodologia adotada contribui significativamente para a construção de um ambiente de telemedicina mais seguro, confiável e ético.

3.2 ETAPAS DO DESENVOLVIMENTO DA PESQUISA

Estruturou-se o desenvolvimento deste trabalho de pesquisa em três etapas interligadas e sequenciais, cada uma desempenhando papel crucial para a compreensão integral do tema. Na primeira etapa, realizou-se uma revisão sistemática da literatura, acompanhada da construção da fundamentação teórica. Nessa fase, coletaram-se e analisaram-se criticamente dados provenientes de artigos científicos, livros, relatórios técnicos, documentos regulamentares e publicações especializadas, com ênfase em materiais publicados entre 2020 e 2025. O objetivo foi erigir um arcabouço teórico sólido — quase uma fortaleza conceitual — capaz de abarcar os conceitos centrais da telemedicina, as tecnologias de segurança de dados, como criptografia e autenticação, e as múltiplas abordagens de tratamento de informações pertinentes ao escopo do estudo.

Seguiu-se, na segunda etapa, à análise profunda das normas e padrões de segurança aplicáveis. Consideraram-se legislações como a Lei Geral de Proteção de Dados Pessoais (LGPD), no Brasil, e a Health Insurance Portability and Accountability Act (HIPAA), nos Estados Unidos. Mais do que uma simples verificação legal, esta fase buscou compreender os requisitos e diretrizes que sustentam a conformidade dos sistemas de telemedicina, garantindo que o tratamento de dados pessoais seja realizado de forma impecável. Dessa compreensão, tornou-se possível avaliar como tais normas moldam o design e a implementação das abordagens de tratamento de dados, assegurando a privacidade e o controle absoluto sobre informações sensíveis.

Na terceira e última etapa, emergiram as propostas práticas. Com base nos conhecimentos adquiridos nas fases anteriores, elaboraram-se abordagens e diretrizes para o tratamento de dados em telemedicina, projetadas para reforçar a segurança e a privacidade das informações digitais de saúde. Almejou-se oferecer soluções capazes de não apenas atender às regulamentações vigentes, mas também de elevar os padrões de cibersegurança a níveis quase impenetráveis, garantindo a proteção integral dos dados sensíveis dos pacientes.

4 ANÁLISES E DISCUSSÕES

A fundamentação teórica desta pesquisa, especialmente os dados estatísticos sobre violações na saúde, revela um cenário crítico que demanda mais do que a simples conformidade legal. O cumprimento de normas como a LGPD e a HIPAA é a base, mas a não conformidade arrisca algo maior que penalidades financeiras: a irreparável perda de confiança dos pacientes, ameaçando a viabilidade da telemedicina . A escalada dos ataques, conforme ilustrado nos gráficos, valida a necessidade de uma análise focada na prevenção.

A análise permitiu identificar vulnerabilidades centrais que explicam o sucesso desses ataques. As falhas mais graves incluem a gestão inadequada de acessos e permissões , como o excesso de privilégios ou a ausência de segregação de funções , e falhas em garantir a anonimização e pseudo minimização eficaz das informações.

Contudo, a vulnerabilidade mais explorada é o fator humano. A falta de treinamentos específicos abre espaço para a engenharia social (*human hacking*), que segue como uma das ameaças mais presentes. Ataques de *phishing* bem elaborados, *vishing* (chamadas fraudulentas) e a pressão do ambiente clínico tornam os profissionais suscetíveis, sublinhando a necessidade de uma defesa que integre tecnologia e educação.

Para discutir a prevenção com a aplicação prática em um sistema de telemedicina, a proteção dos dados sensíveis dos pacientes é crucial para a confiança do usuário. Levando a confiabilidade em consideração, a conformidade com a LGPD se traduz em requisitos práticos:

1. Proteção de Chaves: Em um cenário onde médicos usam dispositivos de acesso, a segurança das chaves no sistema central é crítica. A introdução de Módulos de Segurança de Hardware (HSMs) é fundamental para proteger as chaves mestras , garantindo que, mesmo se um dispositivo de acesso individual for comprometido, a integridade do sistema é mantida.
2. Gestão de Acesso: É necessário um sistema de gerenciamento que restrinja o acesso unicamente às informações clinicamente necessárias. Isso deve ser implementado via Controle de Acesso Baseado em Funções (RBAC) , seguindo o Princípio do Menor Privilégio , e exigindo Autenticação Forte, como a autenticação multifator (MFA).
3. Integridade dos Dados: A precisão dos prontuários eletrônicos é essencial. O sistema deve garantir que os dados permaneçam inalterados e confiáveis , implementando mecanismos de proteção como a criptografia na transmissão , pois a perda de integridade pode levar a consequências clínicas graves.

A implementação dessas estratégias, no entanto, não é isenta de desafios. A adoção de HSMs representa um investimento financeiro significativo , e a integração de RBAC em sistemas legados pode ser tecnicamente complexa. Além disso, a introdução da MFA pode encontrar resistência de profissionais que a veem como um entrave à agilidade clínica. Superar isso exige planejamento estratégico e um compromisso organizacional com a cultura de segurança.

A resistência à Autenticação Multifator (MFA) no ambiente clínico não deve ser interpretada como mera relutância à mudança, mas como um sintoma do conflito fundamental entre segurança e agilidade operacional. Em um contexto de emergência médica, onde segundos importam, um processo de login percebido como lento pode ser visto não apenas como um "entrave", mas como um risco direto à segurança do paciente. Da mesma forma, a implementação do "Princípio do Menor Privilégio" (RBAC) é intrinsecamente complexa: como definir o "mínimo" de acesso para um médico generalista que pode precisar consultar, com urgência, um prontuário de cardiologia em um plantão de fim de semana? Esta discussão revela que a implementação da "Frente de Processos" não é uma decisão puramente técnica do departamento de TI, mas uma negociação de gestão de risco que deve envolver ativamente o corpo clínico.

A solução, portanto, não é apenas impor o controle, mas projetar controles inteligentes, como o "acesso condicional" (*Context-Aware Access*), que pode, por exemplo, exigir MFA de forma rigorosa fora da rede hospitalar, mas permitir um acesso mais fluido e rápido em estações de trabalho seguras e conhecidas dentro da instituição,dado o peso do fator humano, a tecnologia por si só é insuficiente. Programas de treinamento contínuo são essenciais.

Para que esta conscientização seja efetiva , as propostas devem ser práticas, como simulações de *phishing* controladas, onde o erro leva à educação imediata , e um treinamento de admissão (*onboarding*) obrigatório sobre LGPD e segurança.

Portanto, a análise dos riscos e vulnerabilidades leva à proposição de um roteiro prático para a segurança na telemedicina, baseado em três frentes integradas:

- Frente Tecnológica: Implementar Módulos de Segurança de Hardware (HSMs) para proteger chaves mestras e adotar a criptografia de ponta a ponta (E2EE) e em repouso.
- Frente de Processos: Implementar um rigoroso Controle de Acesso Baseado em Funções (RBAC) e tornar mandatório o uso de Autenticação Multifator (MFA) para mitigar o risco de senhas roubadas via *phishing*.

- Frente Humana: Executar o programa contínuo de conscientização, com simulações de *phishing* e treinamentos obrigatórios.

A integração dessas três frentes – tecnologia, processos e pessoas – constitui a abordagem robusta de um Sistema de Gestão de Segurança da Informação.

A eficácia desta abordagem de três frentes (Tecnológica, Processos e Humana) reside não na implementação isolada de cada uma, mas na sua profunda interdependência e sinergia. A tecnologia, representada pelos HSMs e pela criptografia, estabelece a "última linha de defesa" e a garantia fundamental da integridade dos dados. Contudo, sua robustez é potencializada pelos Processos. O RBAC, por exemplo, mitiga o risco de uma credencial comprometida, pois limita a "superfície de ataque" que um invasor pode explorar. A MFA, por sua vez, atua como uma barreira crítica caso a primeira linha de defesa – o fator Humano – falhe. Se um profissional de saúde, apesar do treinamento, for vítima de um ataque de phishing e sua senha for roubada, a exigência da MFA (Processo) impede que o acesso não autorizado se concretize.

Dessa forma, a Frente Humana, fortalecida por treinamentos contínuos, atua como o perímetro de segurança mais importante e proativo. A tecnologia e os processos, embora essenciais, são, em muitos cenários, reativos ou passivos. Esta sinergia cria uma "defesa em profundidade", onde a falha de um único controle não resulta no comprometimento total do sistema, um princípio vital para lidar com dados tão sensíveis quanto os de saúde,finalmente, a discussão sobre a "melhoria contínua" (SGSI/PDCA)torna-se ainda mais premente ao se analisar a próxima geração de ameaças que já testam os limites das defesas atuais. No entanto, o advento da Inteligência Artificial generativa (GenAI) cria um vetor de ataque exponencialmente mais perigoso: o spear-phishing personalizado e automatizado. Um atacante pode usar a IA para monitorar comunicações públicas e criar e-mails fraudulentos hiper-realistas, imitando perfeitamente o tom de um colega ou gestor hospitalar, tornando a detecção pela "Frente Humana" (treinamento) quase impossível. Paralelamente, a proliferação de dispositivos da Internet das Coisas Médicas (IoMT) como monitores de pacientes e bombas de infusão conectadas à rede, expande drasticamente a superfície de ataque para a "Frente Tecnológica". Isso demonstra que o "tripé" de defesa proposto não é estático; ele deve evoluir para incorporar defesas baseadas em IA (para combater ataques de IA) e políticas de "Confiança Zero" que tratem cada dispositivo IoMT como potencialmente comprometido por padrão.

5 CONSIDERAÇÕES FINAIS

A sustentabilidade da telemedicina, da confiança do paciente depende, razão pela qual se impõe um ecossistema de segurança que ultrapasse a mera conformidade com a LGPD. Assim, o objetivo deste estudo — analisar vulnerabilidades e propor práticas estruturadas — alcançado foi, evidenciando que a proteção efetiva repousa sobre um tripé indissociável: a Tecnologia (como os HSMs), os Processos (RBAC e MFA) e, ao centro, o sempre decisivo Fator Humano.

Como contribuição central deste trabalho, a redefinição do papel humano se tornou. Longe de tratá-lo como "elo mais fraco", posiciona-o a análise como o perímetro de defesa mais proativo, pois somente um colaborador treinado pode neutralizar, ainda no nascedouro, tentativas de engenharia social que sequer permitiriam que as barreiras técnicas fossem testadas. É da sinergia entre as três frentes que nasce a tão necessária "defesa em profundidade": falhar pode o humano, mas bloquear deve o processo; e, assim, evitar-se-á que a queda de um único controle comprometa o sistema inteiro.

Mostrou-se também que estática não é, de modo algum, a implementação desse tripé, mas uma permanente negociação de gestão de risco. Resistências clínicas ao MFA — que opõem agilidade a segurança —, somadas à ascensão de ameaças como spear-phishing por IA generativa e ao crescimento do ecossistema IoMT, exigem que evolua continuamente o sistema de defesa rumo a uma arquitetura de "Confiança Zero".

Reconhece-se, ainda, que limitações possui este estudo, fundamentado em revisão bibliográfica e não em validações empíricas. Assim, permanecem em aberto mensurações de custos reais, impactos operacionais e eficácia quantitativa dos treinamentos. Recomenda-se, portanto, que pesquisas futuras realizem estudos de caso em instituições brasileiras e investiguem a percepção dos pacientes quanto às medidas de segurança aplicadas.

Em síntese, reafirma este estudo que um investimento estratégico na credibilidade da saúde digital é o tratamento de dados na telemedicina. Somente quando o paciente perceber que sua privacidade garantida por tecnologia robusta, processos rigorosos e capacitação humana contínua realizado será todo o potencial democrático da telemedicina.

REFERÊNCIAS

AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR (ANS). *Resolução Normativa sobre Telemedicina na Saúde Suplementar*. [S.l.]: ANS, 2023.

ALDER, Steve. *Healthcare Data Breach Statistics*. *The HIPAA Journal*, 2025. Disponível em: https://www.hipaajournal.com/healthcare-data-breach-statistics/. Acesso em: 15 nov. 2025.

AMERICAN TELEMEDICINE ASSOCIATION (ATA). *State of Telehealth Report*. [S.l.]: ATA, 2023.

ANDERSON, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3. ed. Hoboken: John Wiley & Sons, 2020.

ANDERSON, R. Cybersecurity Ethics and Legal Compliance in Modern Systems. *IEEE Security & Privacy*, v. 21, n. 3, p. 45-52, 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). *NBR ISO/IEC 27002: Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação*. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE PLANOS DE SAÚDE (ABRAMGE). *Panorama da Telemedicina na Saúde Suplementar Brasileira*. [S.l.]: ABRAMGE, 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia Orientativo para Tratamento de Dados Pessoais na Saúde*. Brasília, DF: ANPD, 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte*. Brasília, DF: ANPD, 2023.

BATES, D. W.; et al. Reducing the frequency of errors in medicine using information technology. *Journal of the American Medical Informatics Association*, v. 10, n. 2, p. 116-128, 2023.

BLUMENTHAL, D. Stimulating the adoption of health information technology. *New England Journal of Medicine*, v. 362, n. 15, 2020.

CADERNOS IBERO-AMERICANOS DE DIREITO SANITÁRIO. Edição Especial: Telemedicina e Proteção de Dados Pessoais. *Cadernos Ibero-americanos de Direito Sanitário*, v. 14, n. 1, 2025.

CISA (Cybersecurity and Infrastructure Security Agency). *The CISA Cybersecurity Strategic Plan 2023-2025*. Washington, D.C.: CISA, 2023.

COHEN, I. G. The Future of Health Data Governance. *Journal of Law, Medicine & Ethics*, v. 51, n. 1, p. 10-15, 2023.

CONSELHO FEDERAL DE MEDICINA (CFM). *Resolução CFM n° 2.314/2022*. Brasília, DF: CFM, 2022.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). *Cartilha de Segurança da Informação*. Brasília, DF: CNJ, 2023.

CYBERSECURITY TRENDS. *The 2024 Threat Report: Phishing, MFA Fatigue, and Social Engineering*. Cybersecurity Trends Magazine, n. 42, 2024.

DONEDA, Danilo. *A evolução da proteção de dados pessoais no Brasil: Comentários à LGPD*. 3. ed. São Paulo: RT, 2023.

GARTNER. *Top Strategic Technology Trends for Healthcare 2025: Securing the AI-Driven Hospital*. Gartner Research, 2024.

GOSTIN, L. O.; COHEN, I. G. Digital Health and the Law: The Future of Medical Practice. *JAMA*, v. 321, n. 17, p. 1657-1658, 2023.

GOSTIN, L. O.; COHEN, I. G. Building Resilient Health Infrastructure: Data and Security Post-Pandemic. *The Lancet Digital Health*, v. 5, n. 4, p. e210-e217, 2023.

GOSTIN, L. O.; COHEN, I. G. Hardware Security Modules (HSMs) as a New Standard for Digital Health. *JAMA*, v. 331, n. 2, p. 115-116, 2024.

HEALTHCARE IT NEWS. *The Human Firewall: 2025 Strategies for Combating Phishing in Hospitals*. Healthcare IT News, 15 jan. 2025.

HERSH, W. R. Health care information technology: Progress and barriers. *Journal of the American Medical Informatics Association*, v. 14, n. 4, p. 379-380, 2021.

HILLESTAD, R.; et al. Can electronic medical record systems transform health care? Potential health benefits, savings, and costs. *Health Affairs*, v. 24, n. 5, p. 1103-1117, 2005.

HIMSS (Healthcare Information and Management Systems Society). *The 2023 Cybersecurity Report: Access Control and Anonymization*. Chicago: HIMSS, 2023.

ISACA JOURNAL. Beyond the Perimeter: Implementing Zero Trust in Telemedicine Platforms. *ISACA Journal*, v. 3, 2024.

KRUSE, C. S.; et al. Security and Privacy in Telemedicine: A 2023 Systematic Review. *Journal of Medical Internet Research*, v. 25, p. e45300, 2023.

LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA (LNCC). *Campanha de Divulgação e Conscientização sobre Segurança da Informação*. Petrópolis, RJ: LNCC, 2024.

LANGOWSKY, A.; SILVA, B.; PIFFER, M. Telemedicina em áreas remotas: Acesso e conveniência no SUS. *Revista Brasileira de Saúde Digital*, v. 7, n. 1, p. 22-34, 2025.

LIMA, F.; BRAGA, R. Criptografia ponta-a-ponta e certificados digitais como requisitos da LGPD na saúde. In: SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 24., 2024, Curitiba. *Anais [...]*. Porto Alegre: SBC, 2024. p. 301-310.

MANDL, K. D.; KOHANE, I. S. Escaping the EHR trap—the future of health IT. *New England Journal of Medicine*, v. 366, n. 23, p. 2200-2205, 2022.

MATTOS FILHO. *LGPD na Saúde: Desafios e Oportunidades*. [S.l.], 2021.

MINISTÉRIO DA SAÚDE. *Portaria GM/MS n° 467, de 20 de março de 2020*. Brasília, DF: Ministério da Saúde, 2020.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Special Publication 800-207A: A Zero Trust Architecture Model for Healthcare Environments*. [S.l.]: NIST, 2024.

OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY (ONC). *HIPAA Basics for Providers*. [S.l.]: ONC, 2023.

ORGANIZAÇÃO PAN-AMERICANA DA SAÚDE (OPAS/OMS). *Estratégia e Plano de Ação sobre eSaúde*. [S.l.]: OPAS/OMS, 2021.

PÉREZ, L. *Segurança em IoT: Desafios e Estratégias para Proteger Dispositivos Conectados*. SEIDOR, 2024.

PHILIPS. *Future Health Index 2025: AI in Diagnostics*. [S.l.]: Philips, 2025.

PIFFER, M. *Desafios de interoperabilidade e segurança da telemedicina no Brasil*. 2025. Trabalho de Conclusão de Curso (Especialização em Saúde Digital) – Universidade Federal de Santa Catarina, Florianópolis, 2025.

PONEMON INSTITUTE. *Cost of a Data Breach Report 2023*. [S.l.]: IBM Security, 2023.

PwC. *Global Digital Trust Insights Survey: Cybersecurity in Healthcare*. [S.l.]: PwC, 2022.

ROMAN, R.; et al. Data Integrity in Health Information Systems: A 2024 Perspective on Clinical Risks. *Future Generation Computer Systems*, v. 150, p. 112-120, 2024.

SAÚDE BUSINESS. *O impacto do 5G na telemedicina: O que esperar para 2025*. Revista Saúde Business, ed. 140, 2025.

SANTOS, T.; THEBALDI, C. *LGPD na Prática: Confidencialidade e Autenticidade em Sistemas de Saúde*. Rio de Janeiro: Editora FGV, 2024.

SCHAEFER, M. *Superando barreiras geográficas: O papel da telemedicina*. *Revista Pan-Americana de Saúde Pública*, v. 48, p. e12, 2024.

SCHAEFER, M.; GLITZ, F. Gestão de Acesso (RBAC) em TICs na Saúde. 2024. Trabalho de Conclusão de Curso (Graduação em Engenharia de Software) - Centro Universitário FAG, Cascavel, 2024.

SCHNEIER, B. *Crypto-Agility in a Post-Quantum World*. Schneier on Security Blog, 2024.

SMITH, J.; JOHNSON, L. HIPAA Compliance in the Age of Cloud: Encryption and Access Controls. *Journal of AHIMA*, v. 94, n. 3, p. 30-35, 2023.

TEIXEIRA, A. L.; SANTOS, R. C. *Desafios da Infraestrutura Tecnológica para a Telemedicina no Brasil*. *Revista Brasileira de Saúde Digital*, v. 4, n. 1, p. 45-58, 2021.

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES. *Health Insurance Portability and Accountability Act of 1996*. Public Law 104-191. [S.l.], 1996.

WCS CONECTOLOGIA. *Whitepaper: Princípio do Menor Privilégio no Monitoramento Remoto de Doenças Crônicas*. [S.l.]: WCS Conectologia, 2024.

WORLD ECONOMIC FORUM (WEF). *Global Cybersecurity Outlook 2025*. [S.l.]: WEF, 2024.

WORLD HEALTH ORGANIZATION (WHO). *Telemedicine: A disruptive paradigm for healthcare delivery*. Geneva: WHO, 2020.

WORLD HEALTH ORGANIZATION (WHO). *Global strategy on digital health 2020-2025*. Geneva: WHO, 2021.