Interoperabilidade de dados no setor de saúde

maio/ 2024

idec
instituto de defesa de consumidores

idec
instituto de defesa
de consumidores

Introdução[1]

O Idec - Instituto de Defesa de Consumidores é uma organização da sociedade civil brasileira criada em 1987 com o objetivo de defender os direitos dos consumidores, possuindo atuação em sete programas temáticos. Dois deles, os programas de Saúde e de Telecomunicações e Direitos Digitais compõem sua interface de saúde digital, em um esforço para unir os debates sobre proteção de dados pessoais e direito à saúde.[2]

Dentro deste debate tem ganhado notável relevância a necessidade de integração dos sistemas de informação em saúde, com consequente compartilhamento de dados no setor. A integração de dados pode ser utilizada para potencializar a gestão e o acesso à saúde, afinal o tratamento isolado de dados pode ocasionar inferências insuficientes sobre o estado de saúde de um usuário e o Sistema na totalidade. Em contrapartida, o compartilhamento de dados também pode resultar em abusividades e discriminações, especialmente a partir do tratamento de dados de saúde para fins não relacionados à assistência ou não centrados no interesse público.[3] Exemplos desses riscos podem ser identificados nas movimentações mais recentes sobre o tema, como o Projeto de Lei nº 5875/2013[4] e a audiência pública organizada pela Agência Nacional de Saúde Suplementar (ANS) sobre compartilhamento de dados em portabilidade[5].

No atual cenário, a política vigente é a Rede Nacional de Dados em Saúde (RNDS), que, embora tenha dispositivos específicos sobre interoperabilidade, não está devidamente adequada à LGPD - ocasionando riscos ao tratamento de dados pessoais dos usuários.

O Idec compreende que as políticas de interoperabilidade de dados no setor de saúde, seja público ou privado, devem ser focadas na centralidade do usuário, em especial no respeito ao direito à informação, à transparência e na autodeterminação informativa, visando garantir tanto a proteção de dados quanto o direito à saúde. A partir dessas colocações e compreendendo a necessidade de transparência e participação social nessas discussões, o Idec apresenta contribuições quanto à interoperabilidade de dados a partir do policy paper "Agenda de Dados e Saúde: recomendações para uma

---

[1] Este policy briefing foi produzido pela equipe de pesquisadores dos programas de saúde e telecomunicações e direitos digitais do Instituto de Defesa de Consumidores (Idec): Ana Carolina Navarrete, Camila Leite Contri, Marina Fernandes, Marina Paullelli, Marina Magalhães, Lucas Marcon e Lucas Andrietta.

[2] INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. Agenda de Dados e Saúde: recomendações para uma saúde digital inclusiva. 2024. Disponível em: <https://idec.org.br/sites/default/files/agenda-de-dados-e-saude.pdf>

[3] INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR, Ibidem, 2024.

[4] Em dezembro de 2023, a Coalizão Direitos na Rede (CDR), apontou a necessidade de discussão mais aprofundada sobre aspectos técnicos do PL e a necessidade de maior participação no debate. Disponível em: <https://direitosnarede.org.br/2023/12/08/nota-sobre-o-substitutivo-aprovado-pela-ccti-ao-pl-5875-13-e-seus-apensados/>

[5] Em outubro de 2023, a ANS promoveu uma Audiência Pública e uma Consulta Pública para discutir a portabilidade de informações de usuários. Mais informações disponíveis em: <https://www.gov.br/ans/pt-br/assuntos/noticias/sociedade/audiencia-publica-debate-portabilidade-de-informacoes-de-beneficiarios>

Saúde Digital inclusiva”[6] e dos princípios para a Governança de Dados em Saúde (GDSAS)[7].

INTEROPERABILIDADE: GARANTIAS E VEDAÇÕES

Considerando que essas questões são centrais na pauta de saúde e de direitos digitais, o Idec apresenta as seguintes recomendações para que a interoperabilidade de dados no setor de saúde seja focada na centralidade do usuário, protegendo direitos individuais e coletivos.

1. GARANTIAS

Para além da adequação à LGPD, também devem ser garantidas, de forma aos titulares-usuários gozarem os benefícios da interoperabilidade de dados:

1.1. **Controle e histórico de acesso às informações**: usuário deve ter acesso ao histórico de logins que acessaram seus dados e, de forma facilitada, às finalidades que justificam o tratamento de dados;

1.2. **Cartão Nacional de Saúde**: em razão dos riscos associados ao uso do CPF, em especial a triangulação de dados, é preferível que a chave identificadora dos usuários seja o Cartão Nacional;

1.3. **Inteligência Artificial (IA):** no uso de IA deve ser garantida a representação de grupos e populações vulneráveis no treinamento do algoritmo e atenuar o viés dos dados, de maneira a considerar as necessidades específicas de cada grupo;

1.4. **Prazo para que os dados sejam excluídos ou removidos do sistema**: dados de saúde representam o indivíduo em sua natureza imutável, de forma que registros longitudinais prolongam os riscos do tratamento para além do necessário. É necessário que a autoridade responsável estabeleça um prazo máximo para os dados permanecerem no sistema ou uma maneira de renovar sua autorização, desde que respeitadas as obrigações regulatórias e legais médicas, além da proteção da segurança dessas informações e sem o prejuízo do exercício do direito de eliminação de dados (Art. 18, inciso VI).

---

[6] INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR, Ibidem, 2024.

[7] Os Princípios de Governança de Dados Sobre A Saúde foram conduzidos pela Coalizão Transform Health e desenvolvidos pela sociedade civil por um processo inclusivo e consultivo, administrado pela iniciativa entre 2020 e 2022. São eles: I - Proteger Pessoas e Comunidades; II - Construir Confiança nos Sistemas de Dados; III - Garantir a Segurança dos Dados; IV - Melhorar os Sistemas e Serviços de Saúde; V - Promover o Compartilhamento e a Interoperabilidade; VI - Facilitar a Inovação Usando os Dados sobre a Saúde; VII - Promover Benefícios Equitativos dos Dados sobre a Saúde e VIII - Estabelecer Direitos de Propriedade sobre os Dados. Ref: SILVA, Angélica Baptista; SOUZA, Vanessa de Lima. Governança de dados sobre a saúde como direito humano. In: Proteção de Dados Pessoais em Serviços de Saúde Digital. Rio de Janeiro: Fiocruz, 2023.

2. VEDAÇÕES

Políticas de interoperabilidade de dados de saúde devem neutralizar os riscos de captura dos dados pessoais para transformação em ativos econômicos. A economia movida a dados prospera a partir de ideais de exploração econômica dos dados pessoais, especialmente para fins de publicidade e propaganda direcionada, mas também para análises preditivas e discriminatórias que podem comprometer o acesso à saúde.

2.1. Definir usos inadequados de dados de saúde: análises preditivas, como healthscore e perfilização; vigilância não relacionada à saúde, discriminação ilícita e publicidade personalizada, são exemplos de usos inadequados desses dados;

2.2. Cláusula específica de não seleção de risco no setor privado: os dados pessoais não podem ser usados de maneira a trazer desvantagens (sociais e econômicas) ao usuário-titular. É preciso um direcionamento regulatório da ANS para mapear práticas de seleção de risco e construir melhores vedações;

2.3. Restringir o acesso a dados aos prestadores: no caso de interoperabilidade dentro do setor privado, não existe argumento técnico que justifique o acesso aos dados por operadoras de planos de saúde (ou, no caso de empresas verticalizadas, do seu braço administrativo). Em razão dos riscos relacionados à exploração econômica e a seleção de risco a partir de dados detalhados do histórico de saúde do paciente, deve ser vedado o acesso de dados pessoais de saúde as operadoras e a outros entes privados, como plataformas digitais, incluindo dados clínicos, de gestão e até mesmo a metadados;

2.4. Impedir acesso em situações não-necessárias: o tratamento de dados deve corresponder a necessidades específicas, justificáveis e previamente definidas. Com isso, os dados pessoais não devem ser acessados fora do contexto de acesso à saúde, o que inclui, por exemplo, consultas e exame médicos;

2.5. Usos secundários: impedimento da utilização de dados para fins não informados previamente aos seus titulares.

MITIGAÇÃO DE RISCOS A PARTIR DA ADEQUAÇÃO E REGULAMENTAÇÃO DA LGPD NO SETOR DE SAÚDE

Para que a política de interoperabilidade possa aumentar a qualidade da prestação dos serviços, a confiança dos usuários de saúde e empoderá-los no tratamento de seus dados pessoais, é fundamental que os mais altos níveis de proteção de dados sejam garantidos. Qualquer política envolvendo o tratamento de dados deve ser

fundada na compreensão de que o usuário é o titular de seus dados, devendo, portanto, gozar de sua autodeterminação informativa para orientar este tratamento.

1. Adequação e Regulamentação da LGPD

A adequação do setor de saúde à Lei Geral de Proteção de Dados (LGPD) ainda é baixa.[8] Com isso, fica evidente que a política de interoperabilidade deve estar adequada à LGPD e respeitando as futuras regulamentações da Autoridade Nacional de Proteção de Dados (ANPD), sem prejuízo do surgimento de novas normas harmônicas sobre o tema e cooperação entre as autoridades. Nesse sentido, a regulamentação da LGPD em saúde deve seguir as seguintes diretrizes:

1.1. **Transparência e acesso adequado à informação**: os titulares devem ser capazes de compreender a necessidade e finalidade da coleta, a forma como os dados são tratados e quais são seus direitos em relação ao tratamento. Deve-se garantir que a linguagem utilizada seja acessível.

1.2. **Consentimento qualificado (art. 11, inciso I, LGPD)**: o consentimento é a hipótese prioritária para o tratamento de dados sensíveis de saúde. Para que o consentimento seja considerado lícito, ele deve ser livre, informado e inequívoco:

1.2.1. *Livre*: para tanto é necessário analisar (i) a assimetria de poder e se ela impõe uma subordinação; e (ii) quais são as escolhas oferecidas ao titular de dados. Com isso, o consentimento não pode estar atrelado a vantagens irresistíveis aos titulares que lhe retirem seu poder de escolha (ex. coação do consentimento no fornecimento de CPF em farmácia para descontos em produtos e medicamentos). Este requisito é particularmente relevante em se tratando de dados relacionados ao mercado de saúde, caracterizado por uma profunda assimetria de informações entre pacientes e profissionais de saúde, gestores ou vendedores de serviços;

1.2.2. *Informado*: a decisão do titular deve ser subsidiada por informações transparentes, acessíveis e confiáveis para que o consentimento possa ser considerado uma manifestação de vontade consciente;

---

[8] Em 2022, dentre os estabelecimentos com acesso à Internet, apenas 26% publicaram sua política de privacidade em seu website ou no da secretaria de saúde, sendo significativa a diferença entre públicos (19,9%) e privados (31,6%). Sendo que apenas 17% dos estabelecimentos públicos e 34,7% dos privados disponibilizou canais de atendimento e interação com os titulares voltados ao tratamento de dados. Refs: INSTITUTO DE COMUNICAÇÃO INFORMAÇÃO CIENTÍFICA E TECNOLÓGICA EM SAÚDE; INTERVOZES; INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. Proteção de Dados Pessoais em Serviços de Saúde Digital no Brasil. Outubro, 2022. Disponível em: <https://intervozes.org.br/wp-content/uploads/2022/11/resumo_executivo_protecao_de_dados_pessoais.pdf>; NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. Pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros: TIC Saúde 2022. São Paulo: Comitê Gestor da Internet no Brasil, 2023. Disponível em: <https://www.nic.br/media/docs/publicacoes/2/20230803103100/tic_saude_2022_livroeletronico.pdf>

1.2.3. *Inequívoco*: um consentimento inequívoco está atrelado ao princípio da finalidade, segundo o qual todo tratamento deve se basear em um propósito específico e explícito (Art. 6º, inciso I, LGPD), não podendo ser declarado a um tratamento genérico de dados pessoais e nem utilizada para finalidades secundárias, muito menos abusivas (ex: para perfilamento de usuários de saúde).

1.3. Outras bases legais para o tratamento de dados pessoais de saúde (além do consentimento): As demais hipóteses do art. 11 devem estar baseadas no interesse público, ser exceções concretas ao consentimento informado, e ser legais, necessárias e proporcionais. Trata-se de situações em que a ausência de consentimento individual representa riscos à saúde pública.

1.3.1. *Execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos*: destinada aos agentes que atuam no exercício de funções administrativas e tenham como finalidade a atenção a programas ou ações governamentais definidas em instrumento formal;[9]

1.3.2. *Proteção da vida ou da incolumidade física do titular ou de terceiro*: trata-se da hipótese adequada quando o tratamento foi indispensável para garantia da vida;

1.3.3. *Tutela da saúde*: é a hipótese mais relevante no setor de saúde e menos delimitada. É necessário que a ANPD estabeleça critérios e limites claros adaptados ao contexto da prestação de serviços de saúde no Brasil.

1.4. Vedação ao compartilhamento de dados de saúde com objetivo de obter vantagem econômica (LGPD, Art. 11, § 4º): diante dos riscos relacionados ao compartilhamento de dados de saúde, a LGPD veda seu compartilhamento para fins econômicos.

1.5. Anonimização dos dados: é preferível que os dados passem por processos de anonimização ou pseudonimização, especialmente aqueles utilizados para gestão e vigilância em saúde - utilizados exclusivamente como forma de repartir com a sociedade os benefícios advindos do uso dos dados. Também devem ser consideradas preocupações com a possibilidade de reidentificação, inclusive decorrente de desenvolvimento tecnológico (ex. triangulação de dados).

1.6. Aprimorar e padronizar o exercício do direito dos usuários (Art. 18): viabilizando seu exercício da maneira menos friccionada para sua fruição plena.

2. Mitigação de riscos a partir da LGPD

A interoperabilidade deve equilibrar os direitos e garantias individuais com a

[9] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Tratamento de dados pessoais pelo Poder Público. ANPD, 2023. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>

importância do uso de dados para a saúde. Mecanismos de mitigações específicos devem ser criados para grupos ou comunidades em situação de vulnerabilidade.

2.1. **Relatório de Impacto em Proteção de Dados (RIPD) e auditorias (LGPD, Art. 38)**: é necessária uma avaliação de risco do tratamento de dados para identificar e mitigar possíveis danos, em especial riscos à segurança pessoal, aos cuidados insuficientes ou incorretos e a exploração econômica.

2.2. **Revisão de decisões automatizadas (LGPD, Art. 20)**: em se tratando de algoritmos de Inteligência Artificial utilizados no setor de saúde, deve-se garantir sua autoria pública, além da revisão humana;

2.3. **Protocolos de segurança (LGPD, Art. 36)**: os padrões de segurança devem ser robustos e capazes de endereçar os riscos no tratamento de dados (ex. criptografia, definir níveis de acesso, autenticação em dois fatores, anonimização, codificação, prevenção a incidentes de segurança);

2.4. **Accountability (LGPD, Art. 6o, inciso X)**: a autoridade responsável por gerir o programa deve adotar medidas eficazes para o cumprimento de normas de proteção de dados. Para tanto, deve disponibilizar mecanismos capazes de receber demandas e solicitações dos titulares, bem como ser responsabilizada em caso de incidente de segurança e dano aos titulares, usuários ou profissionais, além de ser capaz de prestar contas de maneira transparente e acessível;

2.5. **Responsabilidade objetiva (LGPD, Arts. 42 a 45; CDC, Arts. 12 e 15)**: Em razão da vulnerabilidade e assimetria informacional dos usuários no tratamento de seus dados de saúde, a responsabilidade pela reparação deve observar o regime civil de responsabilidade objetiva;

2.6. **Prevenção a riscos de captura de interesses**: caso a interoperabilidade inclua atores privados, deve ser assegurado que a política não seja desvirtuada para finalidades abusivas, exploratórias ou discriminatórias em malefício aos titulares de dados.

Governança de Dados em Saúde

Políticas de compartilhamento de dados no setor de saúde devem ser acompanhadas de uma política de governança da saúde digital. A governança dos dados envolve a gestão da arquitetura institucional, a integração de sistemas, colaboração e agenciamentos, comunicação e mecanismos de verificação e contestação, fiscalização e responsabilização para se evitar abusos e discriminações.[10]

A Governança de Dados em Saúde deve efetivar a promoção do Direito à Saúde por

[10] SILVA; SOUZA, Ibidem, 2023.

meio da digitalização com as tecnologias sendo usadas para possibilitar o melhor atendimento às populações e em respeito aos direitos à privacidade e à proteção de dados. Garantindo-se, através da centralização do usuário, a equidade e a não discriminação.

Para tanto, deve ser exercida de maneira a serem ouvidos os usuários de saúde e que seus mecanismos sejam regidos pelo princípio de transparência.

Conclusão

A interoperabilidade de dados de saúde pode trazer algumas vantagens para o usuário, mas a maneira como vem sendo discutida levanta diversas preocupações do seu uso abusivo, inclusive em desrespeito à Lei Geral de Proteção de Dados.

Foi apresentado então um roteiro com garantias, vedações e medidas de mitigação de riscos para o eventual desenvolvimento de medidas de interoperabilidade na saúde. Como premissa e princípio geral, há de se ter o usuário de saúde (cidadão, consumidor e titular de dados) no centro dessas políticas, com especial atenção para a não exploração econômica desses dados pessoais sensíveis.