# Rede Nacional de Dados em Saúde: transformação digital na saúde e proteção de dados pessoais

National Health Data Network: Digital health transformation and data protection

|  |  |
| --- | --- |
| Submetido(*submitted*): 25 June 2023 | Andréa Guimarães Gobbato**[[1]](#footnote-2)\***  https://orcid.org/0009-0002-4752-6002  Victor Oliveira Fernandes**[[2]](#footnote-3)\*\***  https://orcid.org/0000-0001-5431-4142 |
| Parecer(*reviewed*): 5 July 2023 |
| Revisado(*revised*): 21 August 2023 |
| Aceito(*accepted*): 22 August 2023  *Artigo submetido à revisão cega por pares* (*Article submitted to peer blind review*)  Licensed under a Creative Commons Attribution 4.0 International |

***Abstract***

**[Purpose]** The National Health Data Network (RNDS) is a national platform for the integration and interoperability of health information. Since 2019 the network has been implemented in Brazil, in the context of the development of initiatives for the digital transformation in health and to be used by public and private health entities. As it is an environment in which health information circulates, it involves processing of personal data that is subject to the General Data Protection Law (LGPD). Notably, it involves the processing of sensitive health data. This article analyzes the context of the emergence of the RNDS and expose its challenges for the protection of personal data, including the analysis of LGPD rules and how some of these rules are related to the implementation of the network.

**[Methodology/approach/design]** The research was carried out in three fundamental phases. The first consisted of reviewing specialized bibliography and documents published by public entities regarding digital transformation in health and the implementation of the RNDS. The second aimed at identifying the legal provisions relating to the protection of personal data applicable to the RNDS. Finally, the third phase consisted of identifying the measures adopted to RNDS be compliant with these legal provisions and its challenges for compliance with LGPD.

**[Findings]** As a result, the article demonstrates that the RNDS, despite representing progress for national digital transformation in health, faces challenges to comply with the LGPD, with regards to the principles for data processing, such as the purpose and transparency principles, information security and prevention, compatibility of the consent-based approach of the RNDS with the requirements for valid consent of the LGPD and the legal prohibition of sharing health data with the objective of obtaining economic advantage.

**Keywords**: National Health Data Network. Digital transformation. Digital health strategy. Data Protection. LGPD. Health data.

**Resumo**

**[Propósito]** A Rede Nacional de Dados em Saúde (RNDS) é uma plataforma nacional de integração e interoperabilidade de informações em saúde. A rede vem sendo implementada desde 2019 no Brasil, no contexto do desenvolvimento de iniciativas para a transformação digital na saúde, e tem como objetivo ser utilizada por entidades públicas e privadas da saúde. Por se tratar de um ambiente em que circulam informações de saúde, ela envolve tratamentos de dados pessoais que estão sujeitos à Lei Geral de Proteção de Dados (LGPD). Envolve, especialmente, o tratamento de dados sensíveis de saúde. Este artigo propõe analisar o contexto de surgimento da RNDS e expor desafios para a proteção de dados pessoais nesse ambiente, o que inclui a análise de normas da LGPD e como algumas dessas normas se relacionam com a implementação da rede.

**[Metodologia/abordagem/design]** A pesquisa foi realizada em três etapas fundamentais. A primeira consistiu na revisão de bibliografia especializada e de documentos publicados por entidades públicas com a temática de transformação digital na saúde e a implementação da RNDS. A segunda buscou identificar os dispositivos legais relativos à proteção de dados pessoais aplicáveis à RNDS. Por fim, a última etapa consistiu na identificação das medidas adotadas para a adequação da RNDS a esses dispositivos legais e os seus desafios para adequação à LGPD.

**[Resultados]** Como resultado, o artigo demonstra que a RNDS, embora represente um avanço na transformação digital em saúde do País, possui desafios para sua adequação à LGPD, os quais incluem o atendimento aos princípios para o tratamento de dados, como os princípios da finalidade e da transparência, a segurança da informação e adoção de medidas preventivas, a compatibilidade da abordagem baseada no consentimento da RNDS com os requisitos para o consentimento válido da LGPD e a vedação ao compartilhamento de dados referentes à saúde com o objetivo de obter vantagem econômica.

**Palavras-chave**: Rede Nacional de Dados em Saúde. Transformação digital. Estratégia de Saúde Digital. Proteção de dados. LGPD. Dados de saúde.

## Introdução

A Rede Nacional de Dados em Saúde (RNDS) é uma plataforma que opera como repositório digital de informações de saúde de pacientes e, gradativamente, está sendo implementada no território nacional. A plataforma foi idealizada para integrar sistemas e para ser utilizada por diversos estabelecimentos de saúde públicos e privados e por órgãos de gestão em saúde dos entes federativos em todo o País.

O surgimento e desenvolvimento da RNDS remonta à transformação digital de sistemas na área da saúde, com o propósito de modernizar as ferramentas utilizadas pelos agentes da área, promover o acesso à saúde e assegurar a prestação eficiente de serviços de saúde aos cidadãos. Considerando que há um grande potencial na aplicação de tecnologias da informação e comunicação para questões de saúde (por exemplo, através do uso de dispositivos, ferramentas, sistemas, sensores de monitoramento, soluções de inteligência artificial, internet das coisas), as ações voltadas à RNDS representam uma parcela dos esforços direcionados à concretização desse potencial.

Ao final da implementação da RNDS, busca-se criar um ambiente de interoperabilidade e interconectividade entre sistemas para melhorar o acesso à saúde e fomentar a inovação. De acordo com o Ministro da Saúde, a criação de um ambiente de *open health* traria benefícios para o setor de saúde brasileiro, público e privado, através do uso de “sistema moderno, eficaz, transparente e que traga mais concorrência ao mercado de planos de saúde”.[[3]](#footnote-4)

Por se tratar de um repositório digital de informações, a RNDS envolve o armazenamento e tratamento de dados pessoais por atores públicos e privados. Por isso, demanda esforços direcionados para a proteção dos dados pessoais e para a adequação à Lei Geral de Proteção de Dados (Lei n° 13.709/2018 ou “LGPD”), que estabelece uma série de regras a serem observadas antes da realização de qualquer atividade que envolva dados pessoais, incluindo o uso compartilhado dos dados entre entidades de saúde e gestores públicos.

Exemplos de medidas de adequação à LGPD incluem o respeito aos seus princípios para o tratamento de dados, a indicação de bases legais, a garantia dos direitos dos titulares de dados, a adoção de medidas eficazes de segurança da informação, entre outras. Ainda, os dados pessoais referentes à saúde são categorizados como dados pessoais sensíveis pela LGPD,[[4]](#footnote-5) o que significa que esses dados estão sujeitos à maior proteção legal, em razão dos potenciais impactos e danos aos indivíduos no caso do uso indevido desses dados.

Tradicionalmente, o setor de saúde processa uma grande quantidade de dados, utilizados para a prestação dos serviços, para aprimorar métodos e técnicas aplicados por diversos agentes, como profissionais de saúde, fornecedores de produtos e serviços, desenvolvedores de produtos e pelos próprios indivíduos isoladamente. Com a evolução tecnológica e a adoção de novas soluções, aumenta-se a possibilidade de coleta e tratamento de dados no ambiente de saúde e também os riscos relacionados ao uso indevido desses dados e por pessoas não autorizadas.

No âmbito da RNDS, um desafio da adequação se refere à concretização da rede como interoperável - a interoperabilidade é um dos pilares da RNDS e está prevista na LGPD como um dos elementos para o uso compartilhado de dados para a execução de políticas públicas.[[5]](#footnote-6) Por um lado, a interoperabilidade fomenta a transformação da prestação de serviços de saúde ao padronizar informações e fornecer maior conectividade aos estabelecimentos. Por outro, ao permitir a conexão entre diferentes sistemas de informação em saúde, requer que sejam definidas regras de acesso e limites de compartilhamento entre os atores envolvidos.

Além disso, conforme será apresentado neste artigo, há outros desafios a serem enfrentados na concretização da rede para que esta cumpra com as regras da LGPD. Entre esses, destacam-se a complexidade para observar os princípios da finalidade e da transparência, a garantia à segurança da informação e a obtenção do consentimento dos indivíduos, quando necessário, em consonância com a referida lei.

O presente artigo tem como objetivo contextualizar a RNDS na transformação digital da saúde e analisar seus desafios para cumprimento com a legislação de proteção de dados no Brasil, notadamente a LGPD. Para tanto, a primeira seção se destina a contextualizar a RNDS, no que se refere (i) à transformação digital em saúde e surgimento da RNDS, e (ii) ao objetivo da RNDS. A segunda seção analisa a proteção de dados no âmbito da RNDS, incluindo (i) o tratamento de dados pessoais e a sujeição da RNDS à LGPD, (ii) as medidas para adequação da RNDS à LGPD, e (iii) os desafios para adequação da RNDS à LGPD. O artigo adota uma abordagem ampla, sem pretender esmiuçar cada aspecto da adequação à LGPD.

### Rede Nacional de Dados em Saúde

### *Transformação digital em saúde e surgimento da RNDS*

O desenvolvimento da RNDS encontra-se no contexto da formulação de iniciativas públicas e estratégias nacionais com o objetivo de modernizar a saúde pública no Brasil.[[6]](#footnote-7) Tais iniciativas incluem a Estratégia da e-Saúde, que propôs uma visão de e-Saúde até 2020 (“Estratégia e-Saúde”),[[7]](#footnote-8) o Plano de Ação, Monitoramento e Avaliação de Saúde Digital para o Brasil, que traça um plano de ação para a saúde de 2019 a 2023 (“PAM&A”),[[8]](#footnote-9) a Estratégia de Saúde Digital para o Brasil, que define objetivos para a saúde digital de 2020 a 2028 (“ESD 28”)[[9]](#footnote-10) e a Política Nacional de Informação e Informática, que define princípios e diretrizes a serem observados pelos setores público e privado (“PNIIS”).[[10]](#footnote-11)

Em 2017, as ações recomendadas pela Estratégia e-Saúde apontaram a necessidade de aprimoramento da governança da informação no SUS e de alinhamento de suas ações. Em geral, as recomendações desta estratégia incluíram (i) a redução da fragmentação das iniciativas do SUS e aprimoramento da governança estratégica da e-Saúde, (ii) o fortalecimento da intersetorialidade de governança de e-Saúde, (iii) a elaboração de um marco legal de e-Saúde no País, e (iv) a definição e implantação de uma arquitetura para a e-Saúde.

Embora o documento não mencionasse explicitamente a RNDS, a concepção de uma rede nacional e interoperável se mostrava decorrente do objetivo de construir uma infraestrutura capaz de fornecer o acesso a informações pelos diversos serviços de saúde em todo território nacional. Com isso, a referida estratégia reforçou a necessidade de adoção de padrões interoperáveis para concretizar uma rede que permitisse a visão integrada e padronizada das informações sobre os pacientes. Nesse sentido menciona que:

A construção de uma infraestrutura de padrões de informática em saúde capaz de garantir a interoperabilidade de serviços e sistemas poderá tanto aproveitar as iniciativas existentes em áreas como as dos sistemas bancários como oferecer modelos inovadores para outras áreas. Tal infraestrutura documentada e publicada representa uma excelente oportunidade de desenvolvimento tecnológico e de apoio à inovação ao evidenciar para os atores da saúde as tendências tecnológicas mais importantes, permitindo que os investimentos públicos e privados sejam focados nas necessidades da e-Saúde.[[11]](#footnote-12)

Em seguida, o PAM&A elenca como objetivo da sua primeira fase a implementação de uma RNDS, no âmbito do programa Conecte SUS, a qual deveria representar uma “plataforma informacional de alta disponibilidade, segura e flexível” e que de modo a favorecer “o uso ético dos dados de saúde, anonimizados quando necessário, permitindo, assim, o surgimento de novos serviços, inovação, pesquisa e desenvolvimento que resultem em benefícios para a população e para o Brasil”.[[12]](#footnote-13)

A fim de iniciar a implementação da RNDS, em 2019, a gestão do Conecte SUS estruturou um projeto piloto para a implementação da RNDS no Estado de Alagoas.[[13]](#footnote-14) A intenção era de que tal projeto permitisse aos envolvidos na formulação e desenvolvimento do Conecte SUS a oportunidade de testar o planejamento da RNDS e refinar sua proposta de expansão para o restante do país.[[14]](#footnote-15) Em relatório final do projeto, o Ministério da Saúde relata que foi necessário revisitar o planejamento do projeto para atender as demandas da pandemia do Covid-19. Nesse sentido, foi redirecionado para permitir a integração de notificações e resultados de exames laboratoriais relacionados ao Covid-19 e para implementar o Portal Conecte SUS Cidadão e o Portal Conecte SUS Profissional, os quais facilitam o acesso aos resultados por cidadãos e profissionais de saúde. Por fim, o relatório do projeto piloto estabelece como meta a expansão da RNDS.[[15]](#footnote-16)

A RNDS foi instituída em 2020, por meio da Portaria n° 1.434 do Ministério da Saúde (“Portaria GM/MS n° 1.434/2020”), que também instituiu o programa Conecte SUS. A portaria dispõe sobre a adoção de padrões de interoperabilidade em saúde, e atribuiu a responsabilidade pela implementação da RNDS ao Departamento de Informática do Sistema Único de Saúde (“DATASUS”),[[16]](#footnote-17) o qual pertence à Secretaria Executiva do Ministério da Saúde e existe desde 1991, com o objetivo de promover a modernização do SUS por meio de tecnologias da informação.[[17]](#footnote-18) Além da implementação, o DATASUS também é responsável pela normatização da integração e interoperabilidade da RNDS.[[18]](#footnote-19)

De forma coordenada com esses andamentos, em 2020, a ESD 28 reconheceu a necessidade de fortalecer, consolidar e ampliar as ações propostas no PAM&A, incluindo as iniciativas relacionadas à expansão da RNDS para todos os Estados do Brasil para que esta alcançasse a abrangência a ela proposta, afirmando-se como nacional, ampla, diversa, segura, confiável e de reconhecido valor para todos os envolvidos.[[19]](#footnote-20) A ESD 28 aprofunda a questão e define demais objetivos da RNDS, como o de oferecer suporte às práticas clínicas, telessaúde e aplicativos e de permitir sua interoperabilidade com sistemas externos, como de saúde suplementar, laboratórios, serviços de farmácia e serviços de telessaúde.

A PNIIS, por sua vez, reforça a caracterização da RNDS como plataforma nacional de integração e interoperabilidade. Também estabelece diretrizes para sua implementação, que incluem o desenvolvimento de ambiente de interconectividade e de um ecossistema de inovação, e as competências de agentes envolvidos na execução da PNIIS (conselhos de saúde, esferas de gestão do SUS, estabelecimentos de saúde, profissionais de saúde e usuários).

### *Objetivo da RNDS*

A RNDS é definida pela Portaria GM/MS n° 1.434/2020 como “uma plataforma nacional de integração e interoperabilidade de informações em saúde entre estabelecimentos de saúde públicos e privados e órgãos de gestão em saúde dos entes federativos”, que tem como objetivo “garantir o acesso à informação em saúde necessário à continuidade do cuidado do cidadão”.[[20]](#footnote-21) Essas informações se referem, de forma geral, a dados relativos à atenção em saúde, vigilância em saúde e gestão em saúde.[[21]](#footnote-22)

Além disso, a ESD 28 propõe que a RNDS seja estabelecida como “a plataforma digital de inovação, informação e serviços de saúde, em benefício de usuários, cidadãos, pacientes, comunidades, gestores, profissionais e organizações de saúde”.[[22]](#footnote-23) A PNIIS reforça essa proposição ao estimular o uso da RNDS como ambiente de conectividade em saúde e laboratório de inovação aberta.[[23]](#footnote-24)

As fases de implementação da RNDS são pautadas pelas prioridades estabelecidas na ESD 28. Tais prioridades incluem a definição e desenvolvimento de marcos legais e regulatórios; a expansão de ferramentas de conectividade; o suporte à prática clínica por meio de serviços, como telessaúde e outros aplicativos; a promoção da interoperabilidade, com a atenção primária à saúde, laboratórios, entre níveis de atenção à saúde, serviços de farmácia, de telessaúde e de regulação ambulatorial; e o fomento à inovação. Em suma, a integração das informações de saúde busca auferir benefícios para os cidadãos, para o sistema de saúde pública, para iniciativas de inovação em saúde e para a saúde suplementar.

Conforme introduzido pela Portaria GM/MS n° 1.434/2020, a RNDS deve ser a via única de interoperabilidade nacional em saúde, sendo que as demais iniciativas nacionais de interoperabilidade em saúde devem convergir para sua arquitetura. Ao que tudo indica, esta abordagem está alinhada com as recomendações da Estratégia e-Saúde para suprir lacunas no sistema de saúde brasileiro, bem como com os demais objetivos e ações definidos nas iniciativas subsequentes para estimular a transformação da prestação de serviços em saúde e para assegurar serviços de qualidade aos seus usuários.

Estudiosos da área da saúde apontam a necessidade de transformar o modo como os serviços de saúde são prestados e de elaborar uma nova estratégia centrada nos pacientes. Conforme defendido por Porter e Lee, a construção de uma plataforma eficiente de tecnologia da informação pode viabilizar a execução de mudanças relevantes para a saúde digital e tornar a prestação dos serviços mais eficientes, por meio da automatização e integração de sistemas e processos.[[24]](#footnote-25)

A concretização dos objetivos da RNDS e dos serviços de saúde a ela integrados como uma forma de fomentar a transformação da saúde ainda está em aberto. O alcance deste resultado provavelmente só será percebido no decorrer das fases de implementação da RNDS e da observância de seus desdobramentos.

### Proteção de dados pessoais na RNDS

#### Tratamento de dados pessoais e sujeição da RNDS à LGPD

Por se tratar de uma rede de informações na área da saúde, a RNDS é um ambiente em que circulam dados pessoais, os quais são definidos pela LGPD como a “informação relacionada a pessoa natural identificada ou identificável”.[[25]](#footnote-26) A LGPD também define tratamento de dados pessoais como qualquer operação realizada com dados pessoais, incluindo a coleta, acesso, transmissão, armazenamento e qualquer outra atividade realizada com os dados.[[26]](#footnote-27) Assim, a RNDS é um ambiente que pressupõe a realização de diversos tratamentos de dados - inserção dos dados do paciente na rede por um profissional de saúde, o acesso a esses dados por profissional diverso daquele que os inseriu, seu armazenamento por um prestador de serviços de armazenamento de informações, entre outros.

Neste contexto, destaca-se a circulação de grande volume de dados pessoais de saúde. Os dados referentes à saúde são inseridos na categoria de dados pessoais sensíveis, de acordo com a definição atribuída pela própria LGPD. Segundo a LGPD, dado sensível é qualquer:

dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, **dado referente à saúde** ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (LGPD, art. 5°, II, grifamos)

Os denominados dados sensíveis recebem proteção especial em razão do seu potencial discriminatório e dos possíveis riscos que apresentam aos direitos e liberdades dos titulares, sobretudo se utilizados de forma indevida. Isso significa que agentes que realizam operações de tratamento com essa categoria de dados estão sujeitos a um regime mais restritivo da lei com maiores obrigações de segurança da informação.[[27]](#footnote-28)

A despeito da confidencialidade das informações no setor de saúde e de obrigações profissionais de sigilo, a LGPD trouxe um novo arcabouço jurídico que deve ser observado pelos agentes do setor de saúde. A LGPD é a primeira lei federal que busca regulamentar a proteção de dados pessoais no Brasil, de forma geral e não setorial, sendo aplicável a entidades públicas e privadas, em meios físicos e digitais.

A integração e interoperabilidade dos sistemas busca permitir que estabelecimentos de saúde públicos e privados e órgãos de gestão em saúde dos entes federativos possam tratar dados pessoais (por exemplo, ao acessar, utilizar, transmitir, fazer uso compartilhado, armazenar os dados, etc). Portanto, entidades e órgãos do setor público, incluindo o SUS e gestores públicos, e do setor privado, incluindo a saúde suplementar, farmácias e laboratórios, devem observar as regras estabelecidas pela LGPD.

#### Medidas para adequação da RNDS à LGPD

Conforme mencionado acima, uma das prioridades da ESD 28 se refere à definição e desenvolvimento de marcos legais e regulatórios, entre os quais se encontra iniciativa relacionada à adequação da RNDS à LGPD. Segundo a ESD 28, as atividades para adequação à LGPD foram iniciadas em 2020 e sua conclusão está prevista para o fim de 2028.

As principais atividades a serem desenvolvidas nessa frente incluem: (i) a identificação dos pontos críticos de alinhamento à LGPD para a expansão da RNDS, (ii) a identificação de modelos de compartilhamento de dados de saúde alinhados à LGPD, (iii) a proposição de modelos robustos de consentimento esclarecido e informado de fácil compreensão, implementação e adesão pelo paciente, e (iv) a proposição de modelos de autenticação, segurança, sigilo e privacidade.[[28]](#footnote-29) Também busca capacitar profissionais de tecnologias da informação e comunicação em temas de proteção de dados e segurança da informação, tendo em vista a concretização dessas atividades.[[29]](#footnote-30)

Antes da publicação da ESD 28, medidas para adequação à LGPD já vinham sendo adotadas por entidades públicas. Em 2019, o Comitê de Informática e Informação em Saúde (“CIINFO”) informou a criação de um Comitê de LGPD relacionado ao DATASUS, bem como aprovou a criação de um Subcomitê de Governança de Dados.[[30]](#footnote-31)

Em documento de 2020, o DATASUS informou estar adotando algumas medidas para adequação da RNDS à LGPD, que incluíam: (i) a definição da abordagem de consentimento da RNDS, (ii) a elaboração de estudo e relatório de avaliação de conformidade da RNDS à LGPD, (iii) cooperação técnica internacional com o Reino Unido, por meio do *Better Health Program Brazil - Prosperity Fund,* (iv) gerenciamento de riscos do programa Conecte SUS, e (v) elaboração de nota conjunta com a Assessoria de Comunicação do Ministério da Saúde para a disponibilização ampla e adequada de informações sobre os direitos dos titulares previstos na LGPD.[[31]](#footnote-32)

Em 2021, foi instituído o Grupo de Trabalho para a implementação da LGPD no âmbito do Ministério da Saúde (“GT-LGPD/MS”).[[32]](#footnote-33) As competências do GT-LGPD/MS incluem (i) a elaboração de proposta de portaria para regulamentar a LGPD no âmbito do Ministério da Saúde, (ii) a elaboração de proposta de Plano de Ação, com respectivo cronograma, fases e ações para a implementação da LGPD, (iii) o gerenciamento da implementação da LGPD, (iv) a proposição de medidas para garantir a implementação da lei, e (v) a adoção de outras providências que julgar necessárias.

Entretanto, em 25 de fevereiro de 2022, foi publicada a Portaria n° 156/2022 que prorrogou, por mais 90 dias, o prazo para apresentação do plano de ação para implementação da LGPD pelo GT-LGPD/MS.[[33]](#footnote-34) Até a elaboração deste artigo, tal plano de ação ainda não fora disponibilizado publicamente.

Uma justificativa apresentada para a mudança e atraso em cronogramas relativos à implementação da RNDS foi o direcionamento das ações governamentais no combate à pandemia do Covid-19, conforme mencionado acima.[[34]](#footnote-35) O sistema de saúde do País, incluindo o SUS, teve que se adaptar para atender à população em estado de calamidade e orquestrar ações nacionais e emergenciais. Segundo informações do governo, quando as ações de combate ao Covid-19 estivessem mais bem estruturadas, o programa Conecte SUS deveria retomar sua estratégia inicial.[[35]](#footnote-36)

O que se vislumbra no momento é que componentes de segurança da informação vêm sendo implementados no âmbito da RNDS, o que é exigido pelos princípios da segurança[[36]](#footnote-37) e da prevenção[[37]](#footnote-38) da LGPD. Embora a lei não estabeleça parâmetros técnicos de segurança, dispõe que os agentes de tratamento de dados “devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”.[[38]](#footnote-39)

A RNDS se propõe a armazenar as informações de saúde dos cidadãos com privacidade, integridade e auditabilidade dos dados, além de promover a acessibilidade e interoperabilidade das informações de forma segura e controlada.[[39]](#footnote-40) Também utiliza a tecnologia *blockchain*[[40]](#footnote-41) para promover a segurança e escalabilidade da rede, de modo que as aplicações de saúde digital devem ser executadas em ambientes descentralizados e seguros.

A integração de sistemas com a RNDS ocorre via uma *Application Programming Interface* (“API”) aberta, disponibilizada pelo Ministério da Saúde e sob responsabilidade do DATASUS.[[41]](#footnote-42) Com isso, os softwares utilizados por estabelecimentos de saúde - como referentes a Prontuários Eletrônicos de Pacientes (“PEP”) - podem se integrar à solução da RNDS em *blockchain*. Para o acesso aos sistemas pelos indivíduos, foram desenvolvidos dois aplicativos: Conecte SUS Cidadão, para acesso pelos cidadãos, e Conecte SUS Profissional, para acesso por profissionais de saúde.[[42]](#footnote-43)

Quanto ao acesso por profissionais de saúde, cabe destacar que este se dá mediante autenticação da Certificação Digital ICP-Brasil de instalações de PEP devidamente habilitadas. O acesso pelos profissionais de saúde deve respeitar o contexto de atendimento, sendo devido quando o profissional atuar em procedimento de saúde do cidadão do qual pretende obter a história clínica disponível nos sistemas.[[43]](#footnote-44)

Com essa infraestrutura, busca-se identificar e permitir a rastreabilidade de todos os profissionais e estabelecimentos que acessaram os dados e documentos. Esta é uma medida relevante de controle e gerenciamento de acessos, que pode ser recorrida em casos de tratamentos indevidos de dados, para fins de identificação dos responsáveis.[[44]](#footnote-45)

Embora a garantia da segurança da informação seja um dever do agente de tratamento previsto na LGPD, ela não encerra todas as obrigações relativas à proteção de dados, de modo que cabe ao poder público, na figura do Ministério da Saúde e do DATASUS e no âmbito do programa Conecte SUS, assegurar a adoção de demais medidas de adequação.

#### Desafios para a adequação da RNDS à LGPD

Há diversos desafios a serem enfrentados para a adequação da RNDS à LGPD, os quais demandam medidas iniciais de adequação, bem como o gerenciamento e a revisão contínuos dessas medidas durante a existência da RNDS. A seguir, serão analisados alguns tópicos que se destacam, mas não esgotam todas as medidas que possam se fazer necessárias.

Um primeiro desafio diz respeito ao cumprimento do princípio da finalidade estabelecido pela LGPD e a interpretação do disposto pela Portaria GM/MS n° 1.434/2020. Segundo o princípio da finalidade, o tratamento de dados deve ser realizado “para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”.[[45]](#footnote-46) A Portaria GM/MS n° 1.434/2020, por sua vez, estabelece que as informações constantes da RNDS podem ser utilizadas para fins (i) clínicos e assistenciais, (ii) epidemiológicos e de vigilância em saúde, (iii) estatísticos e de pesquisas, (iv) de gestão, (v) regulatórios, e (vi) de subsídio à formulação, execução, monitoramento e avaliação das políticas de saúde. Embora os termos utilizados pela portaria sejam abrangentes, são o ponto de partida para a delimitação das finalidades de tratamento.

Outro princípio que se destaca é o princípio da transparência, segundo o qual devem ser disponibilizadas “informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial”.[[46]](#footnote-47) O conteúdo mínimo a ser disponibilizado inclui informações sobre (a) as finalidades específicas dos tratamentos de dados, (b) a forma e duração do tratamento, (c) a identificação dos controladores de dados e suas informações de contato, (d) informações sobre o uso compartilhado de dados e a finalidade, (e) as responsabilidades dos agentes que realizarão o tratamento, e (f) os direitos dos titulares.[[47]](#footnote-48)

Atualmente, o Conecte SUS possui uma política de privacidade que tem como objetivo informar os usuários sobre o funcionamento e as regras do serviço.[[48]](#footnote-49) Ainda que essa política possua trechos imprecisos e de difícil compreensão, representa uma medida de transparência sobre o tratamento de dados.[[49]](#footnote-50) Esse documento, ou outro similar, deve vir a ser atualizado, na medida em que a RNDS se expanda,[[50]](#footnote-51) para assegurar que os cidadãos sejam devidamente informados sobre os tratamentos realizados com seus dados.

Também há um desafio para o desenvolvimento da abordagem baseada em consentimento, conforme previsto entre as prioridades da ESD 28. Em primeiro lugar, porque a LGPD prevê outras bases legais para o tratamento de dados além do consentimento[[51]](#footnote-52) e porque a base legal deve corresponder à finalidade específica do tratamento no caso concreto. Nesse sentido, os tratamentos de dados realizados no âmbito da RNDS podem ser justificados por outra base legal, especialmente em razão de a RNDS ser fruto de uma política pública com quadro normativo específico.

Em segundo lugar, caso o consentimento dos usuários da RNDS seja necessário, deve ser obtido de modo a atender os requisitos da LGPD. Para ser considerado válido, o consentimento deve representar uma manifestação livre, informada e inequívoca da vontade do titular e deve poder ser revogado a qualquer momento.[[52]](#footnote-53) Também deve se referir a finalidades específicas, sendo autorizações genéricas consideradas nulas.[[53]](#footnote-54)

Ainda, no caso dos tratamentos de dados pelo Poder Público, em muitas ocasiões o consentimento não será a base legal mais apropriada, como já salientado pela Autoridade Nacional de Dados Pessoais (“ANPD”), tendo em vista que os dados podem ser necessários para cumprimento de obrigações e atribuições legais.[[54]](#footnote-55) Nesse sentido, a análise da abordagem baseada em consentimento terá o desafio de identificar os casos concretos de uso dos dados em que será necessário e compatibilizá-los com os requisitos da LGPD.

No que se refere às medidas de segurança da informação, há uma preocupação quanto à sua efetividade, em razão de ataques recentes aos sistemas do governo e de possíveis vazamentos de dados pessoais de cidadãos – a exemplo de ataques amplamente noticiados em 2021[[55]](#footnote-56) e 2022.[[56]](#footnote-57) Em 2022, a ANPD chegou a instaurar dois processos administrativos sancionatórios em face do Ministério da Saúde e um em face da Secretaria de Estado da Saúde de Santa Catarina, com o intuito de investigar a ausência de implementação de medidas de segurança e a não comunicação de incidente de segurança.[[57]](#footnote-58) Tais processos ainda não haviam sido concluídos no momento de elaboração deste artigo.

Entre outros exemplos, a RNDS chegou a ficar fora do ar após ataque aos sistemas do Ministério da Saúde[[58]](#footnote-59) e, conforme noticiado pela imprensa, um grupo cibercriminoso alegou que invadiu sistemas do site Gov.br e estaria vendendo um volume massivo de dados online.[[59]](#footnote-60) É importante que medidas de prevenção a danos aos titulares dos dados sejam implementadas e que estas sejam aptas a protegê-los contra qualquer forma de tratamento indevido.

Quanto ao Conecte SUS Profissional, no qual profissionais de saúde podem acessar os dados mediante autenticação pela certificação ICP-Brasil e com devida autorização, ressalta-se que tais concessões de acesso devem ser revisadas periodicamente. Isso porque, em caso de acesso indevido e por pessoas não autorizadas, é possível que um incidente de segurança seja configurado.

Por fim, outro desafio na adequação diz respeito à vedação da LGPD à comunicação ou uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, estabelecida no artigo 11, §4°.[[60]](#footnote-61) Tal vedação é a regra geral estabelecida pela lei e comporta algumas exceções, cuja interpretação é relevante para empresas de tecnologia do setor. Desenvolvedores de software e plataformas que permitem a emissão e gestão de documentos médicos eletrônicos (laudos, relatórios, atestados, prescrições, etc) são relevantes para a transformação digital na saúde e podem acessar dados referentes à saúde no âmbito de seus sistemas.[[61]](#footnote-62) A segurança jurídica na interpretação do referido dispositivo será, portanto, relevante para essas empresas.

## Conclusão

A RNDS surgiu e está sendo implementada no contexto de iniciativas para a transformação digital da saúde no Brasil, com o objetivo de suprir lacunas identificadas no sistema de saúde brasileiro e aprimorar a prestação dos serviços. Sua concepção como plataforma de integração e interoperabilidade visa abranger a saúde em todo o território nacional.

Para além de suprir lacunas, busca-se criar um ambiente de interconectividade e inovação, integrando agentes públicos e privados. Em estágio mais avançado de implementação, pretende-se que a RNDS integre sistemas da saúde pública, na atenção primária da saúde e entre níveis de atenção, e permita a integração com aplicações da saúde suplementar, farmácias, laboratórios, telessaúde e outros serviços de saúde. Após pronunciamentos do Ministro da Saúde, o compartilhamento de dados nesse estágio a ser realizado nesse estágio de implementação vem sendo denominado *open health* pelo mercado, em alusão ao open banking implementado no setor financeiro.

No âmbito da RNDS, ocorrem diversas atividades de tratamento de dados pessoais, como coleta, transmissão, acesso e armazenamento de dados pessoais, sendo que cada uma deve observar as regras estabelecidas pela legislação de proteção de dados. A construção do ambiente de interconectividade pretendido pela RNDS deve considerar que os dados pessoais referentes à saúde são considerados dados sensíveis pela LGPD, uma vez que apresentam maior potencial lesivo e discriminatório aos indivíduos. Assim, os agentes que tratam tais dados pessoais devem adotar medidas de proteção proporcionais aos riscos apresentados pelo tratamento.

Considerando que a LGPD entrou em vigor em 2020, a RNDS deve ser implementada de forma a atender aos dispositivos da lei. Alguns desafios para a adequação da RNDS à LGPD se referem ao modo com que ela atenderá os princípios para o tratamento de dados, como os princípios da finalidade e transparência, à garantia da segurança da informação e da adoção de medidas preventivas à ocorrência de danos aos titulares, à compatibilidade da abordagem baseada no consentimento da RNDS com os requisitos para o consentimento válido da LGPD e à vedação ao compartilhamento de dados referentes à saúde com o objetivo de obter vantagem econômica.

Portanto, a RNDS representa um avanço na transformação em saúde do País e pode gerar benefícios para o sistema de saúde, incluindo para os cidadãos e profissionais de saúde, e para o ecossistema de inovação. A proteção aos dados pessoais deve ser considerada no processo de concretização dessa transformação, a fim de atender aos requisitos legais e estabelecer boas práticas para o setor de saúde no tratamento de dados pessoais.

## Referências Bibliográficas

Ata n° 01/2019 da Reunião Ordinária do Comitê de Informática e Informação em Saúde - CIINFO. Disponível em <https://datasus.saude.gov.br/wp-content/uploads/2020/05/ATA-da-1a-Reuni%C3%A3o-CIINFO-21.10.2019-vers%C3%A3o-FINAL-Assinada.pdf>. Acesso em 05.09.2022.

BARROS, Jacson Venâncio de. et al. Rede nacional de dados em saúde: experiência de interoperabilidade na rede de atenção à saúde. In ***Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos Estabelecimentos de Saúde Brasileiros: TIC Saúde 2019*** [livro eletrônico]. Núcleo de Informação e Coordenação do Ponto BR, 1ª Ed. São Paulo: 2020, p. 99 a 112. Disponível em <https://cetic.br/media/docs/publicacoes/2/20201123084414/tic_saude_2019_livro_eletronico.pdf>. Acesso em 05.09.2022.

DALLARI, Analluza B. ***Interpretação do artigo 11, parágrafo 4° da LGPD no contexto pós-pandemia***.Conjur, 26 de agosto de 2022. Disponível em <https://www.conjur.com.br/2022-ago-26/analluza-bolivar-artigo-11-lgpd-contexto-pos-pandemia>. Acesso em 09.09.2022.

DATASUS. ***Ações para a adequação da RNDS à Lei Geral de Proteção de Dados***. Disponível em <https://www.gov.br/saude/pt-br/assuntos/saude-digital/material-de-apoio/AesparaaAdequaodaRNDSLGPD24.06.2020.pdf>. Acesso em 05.09.2022.

Departamento de Informática do SUS. ***Plano de Ação, Monitoramento e Avaliação da Estratégia de Saúde Digital para o Brasil 2019-2023***. Brasília, 2020. Disponível em <https://www.gov.br/saude/pt-br/assuntos/saude-digital/a-estrategia-brasileira/PlanodeAoMonitoramentoeAvaliao.pdf>. Acesso em 07.09.2022.

IANSITI, Marco; LAKHANI, Karim R. ***The Truth About Blockchain***. Harvard Business Review, Janeiro-Fevereiro 2017, p. 118-127. Disponível em <https://hbr.org/2017/01/the-truth-about-blockchain>. Acesso em 12.09.2022.

LEMOS, Ronaldo. ***O governo brasileiro foi hackeado?*** Folha, 4 de setembro de 2022. Disponível em <https://www1.folha.uol.com.br/colunas/ronaldolemos/2022/09/o-governo-brasileiro-foi-hackeado.shtml>. Acesso em 09.09.2022.

OLIVEIRA, Thais Lucena de; NEVES, Gabriella Nunes; ALMEIDA, Jackeline Neves de; SOUZA-ZINADER, Juliana Pereira de; BARROS, Jacson Venancio de. LGPD e Saúde Pública: a Rede Nacional de Dados em Saúde e a Proteção de Dados Pessoais. In ***LGPD na Saúde***. 1ª Ed. São Paulo: Thomson Reuters Brasil, 2021.

Ministério da Saúde. ***Estratégia de Saúde Digital para o Brasil 2020-2028***. Brasília, 2020. Disponível em <https://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf>. Acesso em 07.09.2022.

Ministério da Saúde. ***Estratégia e-Saúde para o Brasil***. Brasília, 2017. Disponível em <https://www.gov.br/saude/pt-br/assuntos/saude-digital/a-estrategia-brasileira/EstrategiaesaudeparaoBrasil_CIT_20170604.pdf>. Acesso em 04.09.2022.

Ministério da Saúde. ***Relatório Final do Projeto Piloto Conecte SUS em Alagoas: análise dos avanços obtidos no Projeto Piloto entre Outubro/2019 e Junho/2020***. Brasília, 2020 Disponível em <https://bvsms.saude.gov.br/bvs/publicacoes/relatorio_projeto_piloto_conectesus_outubro.pdf>. Acesso em 07.09.2022.

SARLET, Gabrielle Bezerra Sales; FERNANDES, Márcia Santana; RUARO, Regina Linden. A proteção de dados no setor de saúde em face do sistema normativo brasileiro atual. In ***Tratado de proteção de dados pessoais***, p. 490 a 510. Rio de Janeiro: Forense, 2021.

Saúde será conectada em todo Brasil: programa Conecte SUS informatizará as unidades de saúde do país; projeto piloto começa por Alagoas. Brasília: CONASS, 2019. Disponível em <https://www.conass.org.br/saude-sera-conectada-em-todo-brasil/>. Acesso em 07.09.2022.

PORTER, Michael E. LEE, Thomas, H. ***The Strategy That Will Fix Health Care***. Harvard Business Review, Outubro de 2013. Disponível em <https://hbr.org/2013/10/the-strategy-that-will-fix-health-care>. Acesso em 04.09.2022.

QUEIROGA, Marcelo. ***'Open health' é questão de tempo, coragem e decisão***. Folha, 5 de março de 2022. Disponível em <https://www1.folha.uol.com.br/opiniao/2022/03/open-health-e-questao-de-tempo-coragem-e-decisao.shtml>. Acesso em 11.09.2022.

World Health Organization. ***Global strategy on digital health 2020-2025***. Genebra, 2021. Disponível em <https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf>. Acesso em 07.09.2022

World Health Organization. ***eHealth Resolution*** (EB115.R20). Disponível em <https://apps.who.int/gb/ebwha/pdf_files/EB115/B115_R20-en.pdf>. Acesso em 07.09.2022.

World Health Organization. ***eHealth standardization and interoperability*** (WHA66.24). Disponível em <https://apps.who.int/gb/ebwha/pdf_files/WHA66/A66_R24-en.pdf?ua=1>. Acesso em 07.09.2022.

|  |
| --- |
| **Journal of Law and Regulation**  **Revista de Direito Setorial e Regulatório**  ***Contact:***  Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório  Campus Universitário de Brasília  Brasília, DF, CEP 70919-970  Caixa Postal 04413  ***Phone:*** +55(61)3107-2683/2688  ***E-mail:*** [ndsr@unb.br](mailto:ndsr@unb.br)  Submissions are welcome at: <https://periodicos.unb.br/index.php/RDSR> |

1. \*Mestranda em Filosofia do Direito pela Faculdade de Direito da Universidade de São Paulo – USP. Advogada com atuação nas áreas de tecnologia e proteção de dados pessoais. Endereço: Alameda Santos, 2384, apto 12. CEP 01418-200. Cerqueira César. São Paulo – SP. E-mail: [andrea.gobbato@usp.br](mailto:andrea.gobbato@usp.br). [↑](#footnote-ref-2)
2. \*\*Doutor em Direito Comercial pela Universidade de São Paulo – USP. Mestre em Direito, Estado e Constituição pela Universidade de Brasília - UnB.E-mail: [victor.fernandes@idp.edu.br](mailto:victor.fernandes@idp.edu.br). [↑](#footnote-ref-3)
3. No início de 2022, o Ministro da Saúde começou a se referir ao ambiente criado pela implementação da RNDS como open health e a relacioná-lo com o open banking, implementado no setor bancário. Mais informações em <https://www1.folha.uol.com.br/opiniao/2022/03/open-health-e-questao-de-tempo-coragem-e-decisao.shtml>. Acesso em 15.11.2022. [↑](#footnote-ref-4)
4. LGPD, art. 5º, inciso II: “para os fins desta Lei, considera-se dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”. [↑](#footnote-ref-5)
5. LGPD, art. 25: “Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral”. [↑](#footnote-ref-6)
6. No cenário internacional, esforços para estas iniciativas de saúde digital também vêm sendo desenvolvidas. A Organização Mundial da Saúde, em 2005, recomendou que os Estados-membros elaborassem planos estratégicos de longo prazo para desenvolver e implementar serviços e tecnologias voltadas à saúde digital, bem como para adotar mecanismos de colaboração entre agentes do setor. Já em 2013, a OMS aprovou resolução para solicitar que os países considerassem a padronização e interoperabilidade de sistemas, infraestrutura e serviços de saúde digital. Em 2021, publicou uma estratégia global para saúde digital até 2025 (World Health Organization. eHealth Resolution (EB115.R20); eHealth standardization and interoperability (WHA66.24); Global strategy on digital health 2020-2025). [↑](#footnote-ref-7)
7. Ministério da Saúde. Estratégia e-Saúde para o Brasil. Brasília, 2017. Disponível em <https://www.gov.br/saude/pt-br/assuntos/saude-digital/a-estrategia-brasileira/EstrategiaesaudeparaoBrasil_CIT_20170604.pdf>. Acesso em 04.09.2022. A referida estratégia foi aprovada pela Resolução GM/MS n° 19/2017. [↑](#footnote-ref-8)
8. Departamento de Informática do SUS. Plano de Ação, Monitoramento e Avaliação da Estratégia de Saúde Digital para o Brasil 2019-2023. Brasília, 2020. Disponível em <https://www.gov.br/saude/pt-br/assuntosaude-digital/a-estrategia-brasileira/PlanodeAoMonitoramentoeAvaliao.pdf>. Acesso em 07.09.2022. [↑](#footnote-ref-9)
9. Ministério da Saúde. Estratégia de Saúde Digital para o Brasil 2020-2028. Brasília, 2020. Disponível em <https://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf>. Acesso em 07.09.2022. A ESD 28 foi regulamentada pela Portaria GM/MS nº 3.632/2020. [↑](#footnote-ref-10)
10. A PNIIS foi inicialmente instituída pela Portaria GM/MS nº 589/2015. Em 2021, o Ministério da Saúde publicou a Portaria GM/MS nº 1.768/2021, que alterou o Anexo XLII da Portaria de Consolidação GM/MS nº 2/2017 e instituiu a nova PNIIS. [↑](#footnote-ref-11)
11. Ministério da Saúde. Estratégia e-Saúde para o Brasil. Brasília, 2017, p. 47. [↑](#footnote-ref-12)
12. Departamento de Informática do SUS. Plano de Ação, Monitoramento e Avaliação da Estratégia de Saúde Digital para o Brasil 2019-2023. Brasília, 2020, p. 15. [↑](#footnote-ref-13)
13. Disponível em <https://www.conass.org.br/saude-sera-conectada-em-todo-brasil/>. Acesso em 07.09.2022 [↑](#footnote-ref-14)
14. Ministério da Saúde. Relatório Final do Projeto Piloto Conecte SUS em Alagoas: análise dos avanços obtidos no Projeto Piloto entre Outubro/2019 e Junho/2020. Brasília, 2020, p. 10 Disponível em <https://bvsms.saude.gov.br/bvs/publicacoes/relatorio_projeto_piloto_conectesus_outubro.pdf>. Acesso em 07.09.2022. [↑](#footnote-ref-15)
15. Ibid. [↑](#footnote-ref-16)
16. Portaria de Consolidação GM/MS n° 01/2017, art. 254-B. [↑](#footnote-ref-17)
17. Disponível em <https://datasus.saude.gov.br/sobre-o-datasus/>. Acesso em 04.09.2022. [↑](#footnote-ref-18)
18. Portaria de Consolidação nº 1/GM/MS, art. 237, II. [↑](#footnote-ref-19)
19. Ministério da Saúde. Estratégia de Saúde Digital para o Brasil 2020-2028. Brasília, 2020, p. 13. [↑](#footnote-ref-20)
20. Portaria GM/MS n° 1.434/2020, art. 3°, que incluiu o art. 254-A na Portaria de Consolidação GM/MS nº 01/2017. [↑](#footnote-ref-21)
21. Portaria de Consolidação GM/MS nº 01/2017, art. 254-A, §1°. [↑](#footnote-ref-22)
22. Portaria de Consolidação GM/MS nº 01/2017, art. 244-B. [↑](#footnote-ref-23)
23. Portaria GM/MS nº 1.768/2021, art. 10, I. [↑](#footnote-ref-24)
24. PORTER, Michael E. LEE, Thomas, H. The Strategy That Will Fix Health Care. Harvard Business Review, Outubro de 2013. Disponível em <https://hbr.org/2013/10/the-strategy-that-will-fix-health-care>. Acesso em 04.09.2022. [↑](#footnote-ref-25)
25. LGPD, art. 5°, I. [↑](#footnote-ref-26)
26. De acordo com o art. 5°, X da LGPD, tratamento é definido como “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”. [↑](#footnote-ref-27)
27. Por exemplo, a LGPD apresenta bases legais mais restritivas para autorizar o tratamento de dados sensíveis, elencadas no art. 11, e estabelece que os controles realizados pelo agente de tratamento devem considerar a natureza dos dados e os riscos que apresentam para os direitos dos titulares, como previsto no art. 50, §1° e art. 5°, XVII. [↑](#footnote-ref-28)
28. Ministério da Saúde. Estratégia de Saúde Digital para o Brasil 2020-2028. Brasília, 2020, p. 35. [↑](#footnote-ref-29)
29. Ministério da Saúde. Estratégia de Saúde Digital para o Brasil 2020-2028. Brasília, 2020, p. 73. [↑](#footnote-ref-30)
30. Conforme Ata n° 01/2019 da Reunião Ordinária do Comitê de Informática e Informação em Saúde - CIINFO. Disponível em <https://datasus.saude.gov.br/wp-content/uploads/2020/05/ATA-da-1a-Reuni%C3%A3o-CIINFO-21.10.2019-vers%C3%A3o-FINAL-Assinada.pdf>. Acesso em 05.09.2022. [↑](#footnote-ref-31)
31. O documento “Ações para a adequação da RNDS à Lei Geral de Proteção de Dados”, de junho de 2020, encontra-se disponível em <https://www.gov.br/saude/pt-br/assuntos/saude-digital/material-de-apoio/AesparaaAdequaodaRNDSLGPD24.06.2020.pdf>. Acesso em 05.09.2022. [↑](#footnote-ref-32)
32. O Grupo de Trabalho foi instituído pela Portaria GM/MS n° 3.231/2021. Disponível em <https://datasus.saude.gov.br/wp-content/uploads/2021/12/SEI_MS-0023924402-Portaria-GM-3231-22-nov-2021-GT-LGPD.pdf>. Acesso em 05.09.2022. [↑](#footnote-ref-33)
33. Disponível em <https://brasilsus.com.br/wp-content/uploads/2022/03/portaria156.pdf>. Acesso em 05.09.2022. [↑](#footnote-ref-34)
34. “Com esse impulso, a estratégia de implantação da RNDS foi reajustada para ser disponibilizada, de forma integrada e imediata, a todos os estados brasileiros, estabelecendo-se, assim, como ferramenta fundamental para o enfrentamento da pandemia. A plataforma propiciará que os laboratórios de análises clínicas enviem os dados para a RNDS, que vai coletar, processar e disponibilizar esse conteúdo de forma segura e com garantia de privacidade para profissionais, gestores e cidadãos por meio do Portal Conecte SUS”. BARROS, Jacson Venâncio de. et al. Rede nacional de dados em saúde: experiência de interoperabilidade na rede de atenção à saúde. In Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos Estabelecimentos de Saúde Brasileiros: TIC Saúde 2019 [livro eletrônico]. Núcleo de Informação e Coordenação do Ponto BR, 1ª Ed. São Paulo: 2020, p. 107. Disponível em <https://cetic.br/media/docs/publicacoes/2/20201123084414/tic_saude_2019_livro_eletronico.pdf>. Acesso em 05.09.2022. [↑](#footnote-ref-35)
35. Ministério da Saúde. Relatório Final do Projeto Piloto Conecte SUS em Alagoas: análise dos avanços obtidos no Projeto Piloto entre Outubro/2019 e Junho/2020. Brasília, 2020, p. 11 Disponível em <https://bvsms.saude.gov.br/bvs/publicacoes/relatorio_projeto_piloto_conectesus_outubro.pdf>. Acesso em 07.09.2022. [↑](#footnote-ref-36)
36. O princípio da segurança é definido como a “utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão” (LGPD, art. 6°, VII). [↑](#footnote-ref-37)
37. O princípio da prevenção estabelece que devem ser adotadas “medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais” (LGPD, art. 6°, VIII). [↑](#footnote-ref-38)
38. LGPD, art. 46. [↑](#footnote-ref-39)
39. Disponível em <https://www.gov.br/saude/pt-br/assuntos/rnds/a-solucao-tecnologica/a-solucao-tecnologica>. Acesso em 05.09.2022. [↑](#footnote-ref-40)
40. O *blockchain* é uma tecnologia que permite o registro de informações em cadeia, na qual a criação de um novo registro gera um novo bloco nessa cadeia - por isso o nome *blockchain*. Essa tecnologia utiliza criptografia para assegurar a confidencialidade das informações e, como regra geral, não permite a alteração das informações já registradas. Para mais informações, ver IANSITI, Marco; LAKHANI, Karim R. The Truth About Blockchain. Harvard Business Review, Janeiro-Fevereiro 2017, p. 118-127. Disponível em <https://hbr.org/2017/01/the-truth-about-blockchain>. Acesso em 12.09.2022. [↑](#footnote-ref-41)
41. O site do Ministério da Saúde menciona que “a implementação da RNDS se dá por meio da disponibilização de ‘contêineres’ virtuais em nuvens para cada estado da Federação. A aquisição, instalação e manutenção desses contêineres estarão sob a responsabilidade do DATASUS”. Disponível em <https://www.gov.br/saude/pt-br/assuntos/rnds/a-solucao-tecnologica/a-solucao-tecnologica>. Acesso em 09.09.2022. [↑](#footnote-ref-42)
42. BARROS, Jacson Venâncio de. et al. Rede nacional de dados em saúde: experiência de interoperabilidade na rede de atenção à saúde. In Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos Estabelecimentos de Saúde Brasileiros: TIC Saúde 2019 [livro eletrônico]. Núcleo de Informação e Coordenação do Ponto BR, 1ª Ed. São Paulo: 2020, p. 105 e 106. Disponível em <https://cetic.br/media/docs/publicacoes/2/20201123084414/tic_saude_2019_livro_eletronico.pdf>. Acesso em 05.09.2022. [↑](#footnote-ref-43)
43. Ministério da Saúde. Estratégia de Saúde Digital para o Brasil 2020-2028. Brasília, 2020, p. 99 [↑](#footnote-ref-44)
44. “Uma das premissas da RNDS é que todos os acessos aos dados são rastreados, isto é, a RNDS é capaz de identificar de forma inequívoca que dado foi acessado, por qual profissional e estabelecimento de saúde se deu a consulta e quando (data/hora) essa consulta foi realizada. Adicionalmente, considerando que os dados disponibilizados pela RNDS são documentos previamente enviados para RNDS, seja por sistemas hospedados no DATACENTER DATASUS, seja por outros sistemas de informação, cabe ressaltar que também é possível rastrear onde esse documento foi originado e enviado para a RNDS. Para atendimento dessa premissa, optou-se pela tecnologia Blockchain para persistência das informações”. OLIVEIRA, Thais Lucena de; NEVES, Gabriella Nunes; ALMEIDA, Jackeline Neves de; SOUZA-ZINADER, Juliana Pereira de; BARROS, Jacson Venancio de. LGPD e Saúde Pública: a Rede Nacional de Dados em Saúde e a Proteção de Dados Pessoais. In LGPD na Saúde. 1ª Ed. São Paulo: Thomson Reuters Brasil, 2021, p. 164. [↑](#footnote-ref-45)
45. LGPD, art. 6°, I. [↑](#footnote-ref-46)
46. LGPD, art. 6°, VI. [↑](#footnote-ref-47)
47. LGPD, art. 9°. [↑](#footnote-ref-48)
48. ConecteSUS. Política de Privacidade. Disponível em <https://conectesus-paciente.saude.gov.br/>. Acesso em 09.09.2022. [↑](#footnote-ref-49)
49. Por exemplo, em seção referente a “Quem realiza o tratamento de dados (Operador)?”, as informações disponibilizadas aos usuários incluem os seguintes dizeres: “Para o serviço Conecte SUS, o Controlador Ministério da Saúde também atua como operador, ou seja, além de ser responsável pelas decisões referentes ao tratamento de dados pessoais, também realiza o tratamento de dados pessoais. O Conecte SUS compartilha dados com uma empresa terceirizada, desenvolvedora da aplicação, sendo assim, é um operador de dados. Todos os controles administrativos e lógicos de segurança foram exigidos à empresa terceirizada”. Este tópico não apresenta clareza suficiente para informar devidamente o cidadão. [↑](#footnote-ref-50)
50. Por exemplo, a referida política de privacidade declara, entre outras informações, que os dados pessoais dos usuários podem ser compartilhados com Secretarias Estaduais e Municipais de Saúde, Agência Nacional de Vigilância Sanitária, a Controladoria-Geral da União, o Tribunal de Contas da União, o operador que desenvolve o Conecte SUS e o serviço de nuvem que armazena os dados. [↑](#footnote-ref-51)
51. As bases legais para o tratamento de dados pessoais são elencadas no art. 7° da LGPD e para o tratamento de dados pessoais sensíveis no art. 11 da LGPD. [↑](#footnote-ref-52)
52. LGPD art. 5°, XII e art. 8°, §5°. [↑](#footnote-ref-53)
53. LGPD, art. 8°, §4°. [↑](#footnote-ref-54)
54. ANPD. Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público. Brasília, 2022, p. 7. Disponível em <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_tratamento_de_dados_pessoais_pelo_poder_publico___defeso_eleitoral.pdf>. Acesso em 07.07.2023 [↑](#footnote-ref-55)
55. ANDRADE, Henrique. Site do Ministério da Saúde sofre ataque hacker durante madrugada e sai do ar. CNN Brasil. São Paulo, 10 de dezembro de 2021. Disponível em <https://www.cnnbrasil.com.br/nacional/site-do-ministerio-da-saude-sofre-ataque-hacker-durante-madrugada-e-sai-do-ar/>. Acesso em 09.09.2022. [↑](#footnote-ref-56)
56. ROCHA, Lucas; FIGUEIREDO, Carolina. Sistemas do Ministério da Saúde estão fora do ar após tentativa de invasão. CNN Brasil. São Paulo, 17 de maio de 2022. Disponível em <https://www.cnnbrasil.com.br/saude/sistemas-do-ministerio-da-saude-estao-fora-do-ar-apos-tentativa-de-invasao/>. Acesso em 09.09.2022. [↑](#footnote-ref-57)
57. BRASIL. Autoridade Nacional de Proteção de Dados. ANPD divulga lista de processos sancionatórios. Brasília, 23 de março 2023. Disponível em <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-lista-de-processos-sancionatorios>. Acesso em 07.07.2023. [↑](#footnote-ref-58)
58. Em reportagem do G1 de 10.01.2022, “o ataque cibernético que derrubou os sistemas do [Ministério da Saúde](https://g1.globo.com/tudo-sobre/ministerio-da-saude/) completa um mês nesta segunda-feira (10) e o acesso à informação ainda é restrito. O principal sistema ainda não voltou a funcionar. É a chamada Rede Nacional de Dados em Saúde, conhecida por ser a “plataforma-mãe”, que reúne todas as informações registradas por estados e municípios, na ponta do Sistema Único de Saúde (SUS)”. Disponível em <https://g1.globo.com/tecnologia/noticia/2022/01/10/ataque-aos-sistemas-do-ministerio-da-saude-completa-1-mes-nesta-segunda-o-acesso-a-informacao-ainda-e-restrito.ghtml>. Acesso em 09.09.2022. [↑](#footnote-ref-59)
59. LEMOS, Ronaldo. O governo brasileiro foi hackeado? Folha, 4 de setembro de 2022. Disponível em <https://www1.folha.uol.com.br/colunas/ronaldolemos/2022/09/o-governo-brasileiro-foi-hackeado.shtml>. Acesso em 09.09.2022. [↑](#footnote-ref-60)
60. O art. 11, §4° estabelece que “é vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: I - a portabilidade de dados quando solicitada pelo titular; ou II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo”. [↑](#footnote-ref-61)
61. DALLARI, Analluza B. Interpretação do artigo 11, parágrafo 4° da LGPD no contexto pós-pandemia Conjur, 26 de agosto de 2022. Disponível em <https://www.conjur.com.br/2022-ago-26/analluza-bolivar-artigo-11-lgpd-contexto-pos-pandemia>. Acesso em 09.09.2022. [↑](#footnote-ref-62)