Prefeitura da Cidade do Rio de Janeiro
Conselho Municipal de Proteção de Dados Pessoais e da Privacidade

Interoperabilidade de dados na Saúde Pública

Medidas e Salvaguardas para implementação respeitando a proteção de dados e privacidade dos titulares

Ano 2024

Prefeitura da Cidade do Rio de Janeiro
Conselho Municipal de Proteção de Dados Pessoais e da Privacidade

Interoperabilidade de dados na Saúde Pública – Medidas e Salvaguardas para implementação respeitando a proteção de dados e privacidade dos titulares

Composição:

1- Alessandra Almeida Lapa
2- Carlos Alexandre
3- Fernando Bourguy
4- Horrara Moreira
5- Walter Gaspar
6- Rafael Barboza
7- Vitor Paludetto

Relatora:
Alessandra Lapa

Sumário

1. Introdução

De acordo com a Constituição de nosso país, a saúde é direito de todos e dever do Estado. Por isso na criação do SUS – Sistema Único de Saúde – foi atendido este princípio constitucional. Uma composição e união das três esferas federativas, Federal, Estadual e Municipal, buscando atender a população brasileira em todos os seus aspectos. Os serviços são amplos, envolvendo atenção primária, média e de alta complexidade, nos serviços de urgência e emergência, atenção hospitalar, ações e serviços de vigilâncias epidemiológicas, sanitária, ambiental e assistência farmacêutica. Essa universalização, equidade e integralidade deverão trazer um atendimento para todos os brasileiros de forma igual e contemplando todos os serviços.

O objetivo desse Relatório é trazer a problemática sobre as vantagens da interoperabilidade de sistemas de saúde para melhor prestação do serviço de saúde pública, porém, sem deixar de levar em conta a dimensão da privacidade e proteção de dados dos indivíduos, propondo medidas e salvaguardas para viabilizar o uso da integração dos sistemas em prol da maior efetividade da execução das políticas públicas de saúde sem ferir o direito fundamental à proteção de dados.

Para tanto, se faz necessário entender o contexto de privacidade e de interoperabilidade, apresentando os desafios e vantagens dessa integração de informações de saúde, evidenciando a aplicação dentro da estrutura da saúde pública municipal do Rio de Janeiro.

Diante desses desafios, foram percebidos quatro grandes critérios deveriam ser abrangidos por uma visão da governança de dados de saúde no setor público que busque coordenação entre a garantia do direito à saúde e à proteção de dados: A localização, a acessibilidade, a interoperabilidade e a reutilização das informações necessárias aos serviços oferecidos.

No contexto atual do Sistema Único de Saúde, abrangidos pela Prefeitura Municipal do Rio de Janeiro, nos atendimentos dos usuários que localizarem, usarem, analisarem e compartilharem dados pessoais dos titulares, sem levar em conta as pesquisas acadêmicas de saúde, foi criada uma necessidade clara de controle e tratamento de diversos dados pessoais e sensíveis da população carioca.

É possível que a relação entre a vasta quantidade de dados de saúde produzidos, coletados e tratados não corresponda plenamente às medidas e

salvaguardas aplicadas para garantir a privacidade e proteção desses dados. Desde a ausência de regulamentação específica na área da saúde, visto que a Lei Geral de Proteção de Dados, Lei nº 13.709 de agosto de 2018 traz para o ordenamento jurídico nacional somente diretrizes gerais, até mecanismos de segurança da informação capazes de mitigar os riscos do tratamento desses bancos de dados sensíveis. “A investigação em novas ferramentas de proteção da privacidade dos dados é tão importante quanto o aumento da quantidade e técnicas mais sofisticadas de recolha de dados sobre indivíduos”.[1]

Quando falamos da Administração Pública, ainda temos outra camada acrescentada a esse contexto: a falta de integração dos bancos de dados utilizados no âmbito da gestão das políticas públicas relativas à saúde pública eles dentro do próprio município, ou com outros entes estaduais e federais e entidades privadas que auxiliam na prestação de serviços de saúde pública.

A interoperabilidade de dados de saúde é uma prioridade na transformação digital, pois e está prevista como Estratégia de Saúde Digital para Brasil 2020-2028[2]. Ela permitiria a troca eficiente de informações entre diferentes sistemas e instituições de saúde, facilitando o acesso a dados clínicos pelos profissionais e melhorando o cuidado ao paciente.

Pensar em interoperabilidade é entender que isso implica na capacidade de dois ou mais sistemas de informação funcionarem juntos, transferirem e utilizarem bancos de dados uns dos outros. Essa integração traz consigo a possibilidade de ganho, no caso da saúde pública, da visualização de uma visão geral do histórico do paciente e melhor prestação do serviço de saúde, analisando a saúde do paciente de forma integrada; porém, também pode acarretar uma eventual redução da privacidade individual do paciente.

A crescente digitalização e integração de sistemas faz surgir desafios importantes relacionados à privacidade e proteção de dados, principalmente no que diz respeito aos dados sensíveis dos pacientes. Um dos desafios que pode ser observado é a maior disponibilidade dos dados utilizados para a prestação de políticas públicas de saúde, uma vez que um número maior de agentes públicos terão acesso aos dados contidos em bancos de dados compartilhados, trazendo a necessidade de se construírem

[1] LOPES, Secundino. QUARESMA, Rui.
[2] https://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf

rigorosos controles de acesso e políticas de privilégios mínimos, baseadas no princípio 'need-to-know'. É importante destacar que a própria Lei do Governo Digital estabelece em seu art. 38, I, que os órgãos e as entidades responsáveis pela prestação digital de serviços públicos deverão gerir suas ferramentas digitais, considerando a interoperabilidade de informações e de dados, respeitados as restrições legais, os requisitos de segurança da informação e das comunicações, as limitações tecnológicas e a relação custo-benefício da interoperabilidade. Portanto, a legislação federal já destaca a necessidade de se avaliar o custo benefício da interoperabilidade, respeitando-se as restrições decorrentes de legislação e das boas práticas em segurança da informação.

O desafio da interoperação desses dados é garantir que todos os usuários dos sistemas exerçam uma consciência clara de sua importância e de seus deveres e responsabilidades em relação ao tratamento de dados pessoais. Isso se traduz em medidas organizacionais e técnicas relacionadas aos princípios básicos da proteção de dados pessoais, fundamentados na autodeterminação informacional e privacidade, assim como os fundamentos da segurança da informação, confidencialidade, integridade e disponibilidade.

Assim ao buscar a implementação de mecanismos de interoperabilidade de bases de dados do sistema municipal de saúde pública, a Prefeitura do Rio de Janeiro deverá se guiar pelas seguintes diretrizes abaixo:

- Transparência sobre a estruturação do sistema e fluxos de dados;
- Visão geral de todas as categorias de dados pessoais e sensíveis armazenados;
- Eliminação dos dados pessoais e sensíveis sob requisição, quando coletados com base no consentimento, salvo hipóteses de guarda de dados previstas em lei, bem como quando esgotada a finalidade original de tratamento;
- Cumprimento da obrigação de prestação de informação;
- Restrição no processamento e acesso somente a pessoal autorizado com níveis de perfil e especialidade;
- Criação de sistema de rastreabilidade, documentado no diretório de processamento;

- Estabelecer uma política de privilégios mínimos, com camadas de autorização de acesso somente ao necessário para o atingimento da finalidade perseguida.

Assim, a Secretaria Municipal de Saúde poderá acompanhar todos os processos, seja de coleta, processamento, armazenamento ou segurança de dados pessoais e sensíveis dos usuários da saúde pública carioca.

2. Apresentação do problema

2.1 Privacidade e proteção de dados na saúde

Na era da Indústria 4.0[3], a privacidade e a proteção de dados tornaram-se questões centrais, tendo em vista o fluxo massivo de dados em todos os ramos, mas, especialmente, no setor da saúde. O avanço tecnológico permitiu um crescimento exponencial na criação, armazenamento e compartilhamento de dados de saúde, levantando preocupações sobre como essas informações são tratadas, quem tem acesso a elas e quais são as medidas e salvaguardas para mantê-las seguras.

Dados pessoais referentes à saúde são valiosos. Para os pacientes e profissionais de saúde, eles constituem um insumo para diagnósticos e terapias, em busca de cura. Não obstante, ao revelarem características biológicas ou psicológicas dos titulares, também abrem as portas para a esfera mais íntima do indivíduo, que muitas vezes ele não revela nem mesmo a familiares.

Se por um lado, tais características servem para a cura, por outro podem revelar vulnerabilidades exploráveis por terceiros mal-intencionados. Além de discriminações abusivas contra pessoas, pela simples razão de serem portadoras de doenças, outros riscos se apresentam. Por exemplo, empresas de seguros podem explorar os dados para negar serviços a quem apresente alto risco de doenças graves; cibercriminosos podem valer-se de vergonhas para extorquir pessoas psicologicamente fragilizadas por doenças; indústrias farmacêuticas podem se apropriar de peculiaridades

[3] O conceito acadêmico de **Indústria 4.0** refere-se à quarta revolução industrial, que integra tecnologias digitais e ciberfísicas nos processos produtivos, caracterizada pela automação avançada, conectividade em tempo real e o uso de dados massivos para otimização da produção. Ela está centrada na convergência de sistemas físicos com sistemas digitais e biológicos, resultando em fábricas inteligentes e autônomas. De acordo com **Hermann, Pentek e Otto (2016)**, a Indústria 4.0 pode ser definida como a digitalização da indústria baseada em "**sistemas ciberfísicos**" (CPS), que envolvem a interconexão de máquinas, produtos e sistemas para a otimização autônoma de processos. Esses sistemas são orientados por dados, utilizam a Internet das Coisas (IoT), computação em nuvem, inteligência artificial (IA) e Big Data para tomar decisões baseadas em análises preditivas.

biológicas para obter lucro isoladamente, como no caso das Mo-Cells[4], ou, numa hipótese extrema, até inocular patologias propositalmente. Por isso, a proteção desses dados é crucial não só para preservar a privacidade dos indivíduos, mas também para garantir a confiança no sistema de saúde como um todo

Em razão de tais riscos, o sigilo médico faz parte do milenar Juramento de Hipócrates[5] e foi incorporado, atualmente, na normatização da proteção de dados pessoais.

Na principal fonte do direito comparado, por exemplo, o Regulamento Geral de Proteção e Dados da União Europeia (GDPR), trouxe normas específicas para os dados de saúde, qualificados dentre as categorias especiais de dados pessoais. Nesse sentido, proibiu seu tratamento, exceto em limitadas exceções, como mediante o consentimento explícito do titular, realização de procedimentos médicos, emergências ou razões de saúde pública. Ademais, impõe, entre outras obrigações, a minimização dos dados, transparência e direito de acesso, adoção de medidas de segurança adequadas, responsabilização das instituições e ainda o direito à portabilidade, dando mais autonomia e controle ao titular sobre seus dados de saúde.

A propósito, o GDPR traz conceito expresso de dado pessoal referente à saúde, que pode ser aproveitado pelo Município do Rio de Janeiro em suas definições:

> "Art. 4º, 15): (...) dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde."

Similarmente, no Brasil, os dados de saúde são categorizados como dados sensíveis. Essa categorização tem o objetivo de dar-lhes maior proteção, uma vez que incidentes de segurança podem produzir efeitos especialmente severos para os titulares envolvidos. Nessa esteira, as bases de tratamento para os dados sensíveis, previstas no art. 11 da LGPD, são mais restritivas em relação ao tratamento de dados pessoais em geral.

Notadamente, estão excluídas hipóteses de tratamento voltadas a interesses particulares. O legítimo interesse e a proteção ao crédito não são fundamentos válidos

[4] https://embryo.asu.edu/pages/moore-v-regents-university-california-1990
[5] "Aquilo que no exercício ou fora do exercício da profissão e no convívio da sociedade, eu tiver visto ou ouvido, que não seja preciso divulgar, eu conservarei inteiramente secreto."

para o tratamento de dados referentes à saúde. Já a execução de contratos também foi restringida e substituída pelo “exercício de direitos, inclusive em contrato”.

Ademais, a LGPD trouxe regras específicas para os dados referentes à saúde em seu art. 11, §4º O dispositivo estabelece forte limitação à circulação dessas informações entre agentes de tratamento com o objetivo de lucro. Originariamente, seu compartilhamento era admitido apenas mediante consentimento ou pedido de portabilidade. Contudo, tal restrição praticamente inviabiliza a operação de hospitais e planos de saúde numa economia de mercado, que dispõe de serviços terceirizados de alta especialização. Diante dessa dificuldade, MP nº 869/18 admitiu a possibilidade de diferentes agentes de tratamento envolvidos em serviços de saúde poderem compartilhar dados para viabilizar suas transações financeiras e/ou administrativas.

Em âmbito público, o tratamento de dados pessoais referentes à saúde permanece admitido para fins de cumprimento de obrigações legais e/ou regulatórias e de execução de políticas públicas, pela Administração Pública, previstas em leis e/ou regulamentos. Entretanto, tais autorizações não concedem uma carta em branco ao Estado para utilizar quaisquer dados para quaisquer fins, bastando uma lei ou regulamento. O próprio Estado está subordinado à LGPD e deve, na elaboração de normas deste tipo, respeitar seus princípios e elaborar relatórios de impacto à proteção de dados pessoais. O tratamento de dados pessoais referentes à saúde também é admitido para órgãos de pesquisa e estudos em saúde pública, respeitadas as obrigações do art. 13 da LGPD. Contudo, pesquisas em saúde comportam certo risco à proteção de dados pessoais, especialmente se valerem-se de dados públicos. Por exemplo, estudos realizados pela Arizona University podem ter violado a privacidade de membros da tribo indigena Havasupai, ao extrapolarem os limites do consentimento obtido[6]. Ocorre que é da natureza de pesquisas em saúde revelarem fatos desconhecidos, que a direcionam para diferentes e inesperadas linhas. Esta natureza dinâmica defronte da rigidez da LGPD pode trazer complicações na gestão do consentimento respectivo.

2.2. Legislação no Brasil sobre interoperabilidade de dados

[6] https://pmc.ncbi.nlm.nih.gov/articles/PMC5310710/

Em 2020, foi instituída a Rede Nacional de Dados em Saúde (RNDS) como plataforma de interoperabilidade em saúde. A iniciativa conjunta do Departamento de Informática do SUS (Datasus) e da Secretaria Executiva do Ministério da Saúde faz parte de um projeto estruturante do Conecte SUS programa do Governo Federal para transformação da saúde digital no país.

Por iniciativa do Conselho Nacional de Saúde, em 2021, foi criada a Política Nacional de Informação e Informática (PNIIS), que estabelece princípios e diretrizes para integrar sistemas de informação em saúde nos setores público e privado.

Além disso, em 2024, o Ministério da Saúde instituiu o Programa SUS Digital, com o objetivo principal de estabelecer diretrizes que possibilitem a promoção do acesso da população às ações e serviços do SUS por meio da transformação digital.

O Ministério da Saúde, através da Secretaria de Informação e Saúde Digital (SEIDIGI), finalizou o repasse de R$ 232 milhões da Primeira Etapa de Adesão do Programa SUS Digital, aos estados e municípios participantes. Desse total, R$ 69,6 milhões foram destinados aos 26 estados e ao Distrito Federal, e R$ 162,4 milhões aos 5.567 municípios, abrangendo 99,9% de toda a rede.

Além disso, o Conselho Federal de Medicina (CFM) e a Agência Nacional de Saúde Suplementar (ANS) regulam o uso de tecnologia na saúde, estabelecendo regras para troca de informações médicas e práticas de segurança da informação.

Atualmente, o Congresso Nacional discute um projeto de lei, em análise na Comissão de Saúde da Câmara dos Deputados e sob relatoria da Deputada Federal Adriana Ventura (NOVO/SP), que trata da criação de um prontuário eletrônico único e interoperabilidade de dados em saúde. O texto pode consolidar em lei federal as regras infralegais e estruturas que tratam sobre a RNDS, a Plataforma SUS Digital e o Cadastro Nacional de Pessoas para a Saúde (CadSUS).

A própria LGPD dispõe em seu art. 257 sobre a necessidade de se manter os dados em formato interoperável e estruturado para o uso compartilhado quando tratados pelo Poder Público.Isso possibilita a execução de políticas públicas, a prestação de serviços públicos, a descentralização da atividade pública e a disseminação ao acesso das informações pelo público em geral.

[7] “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”.

Também vale destacar que poder público não pode transmitir os dados a entidades privadas, salvo em caso de execução descentralizada que exija a transferência, exclusivamente para esse fim específico e determinado; quando houver previsão legal, convênio, contrato que respalde a ação; ou quando a transferência objetivar a prevenção de irregularidades, a proteção, a segurança e a integridade dos dados (art. 26, LGPD). [8]

Trindade (2021), analisando a regulação do *open banking* no Brasil, destaca como está baseada no trinômio portabilidade-interoperabilidade-proteção de dados. A portabilidade, direito do titular de dados pessoais que o permite transferir dados a outros fornecedores de produtos ou serviços (art. 18, LGPD), é intimamente conectada à interoperabilidade. Ambos têm o caráter de operacionalizar o fluxo de dados entre diferentes controladores e operadores em atenção às necessidades da atividade de tratamento ou à vontade manifesta do titular. Assim, são elementos que contribuem para a consecução de alguns fundamentos da disciplina de proteção de dados conforme ditados pelo art. 2º da LGPD, especialmente o da autodeterminação informativa (inciso II) e do desenvolvimento econômico e tecnológico e inovação (V) (TRINDADE, 2021).

Poderíamos, ainda, argumentar que têm papel importante na consecução do princípio da eficiência na Administração Pública (art. 37, CFRB/88), visto que contribuem para a efetiva integração de sistemas eletrônicos. Para completar o trinômio, a proteção de dados serve como elemento basilar para a consecução daqueles dois elementos, assentando a portabilidade e a interoperabilidade firmemente sobre o eixo do livre desenvolvimento da personalidade e a dignidade (art. 1º; art. 2º, VII, LGPD).

Retomando o caso do *open banking*, cumpre destacar que se trata de iniciativa direcionada não apenas à eficiência de sistemas e garantia da autodeterminação do titular de dados, mas também à higidez do ambiente concorrencial em um contexto de economia de plataformas, pois tem o potencial de reduzir barreiras à entrada e enriquecer o sistema de inovação em torno de determinados conjuntos de dados interoperáveis. É interessante destacar que a adesão do titular de dados ao sistema de *open banking*, que em essência conecta *application programming interfaces* (APIs, interface de programação de aplicativos) de variados provedores de serviços financeiros, é baseada em uma manifestação prévia de consentimento livre, informado e inequívoco por meio eletrônico.

[8] FANTONELLI, Miliane. CELUPPI, Ianka Cristina. OLIVEIRA, Fernanda Maia. BURIGO, Fernando. DALMARCO, Eduardo Monguilhott. WAZLAWICK, Raul Sidnei. Lei geral de proteção de dados e a interoperabilidade na saúde pública. J Health Inform. .2020 p.166-171.

Isto se dá em razão de diversos instrumentos normativos, começando pela Lei Complementar nº 105/2001 e a Resolução nº 3401/06 do Conselho Monetário Nacional, que tratam, respectivamente, do sigilo de operações bancárias e da disponibilização de informações cadastrais a terceiros – ambas requerendo autorização explícita do cliente para a transmissão das informações. Estes instrumentos seriam complementados por uma série de desenvolvimentos normativos, incluindo, com destaque, a Lei Geral de Proteção de Dados e a Resolução Conjunta do Banco Central do Brasil e Conselho Monetário Nacional regulamentando o processo de implementação do *open banking* no país (TRINDADE, 2021).

"Ao longo dos últimos anos, o Brasil vem avançando significativamente na implementação de estratégias e padrões para melhorar a interoperabilidade, mas enfrenta desafios devido à fragmentação de sistemas e falta de padronização, além das desigualdades em termos de conectividade e digitalização nas diversas regiões do país", diz Wislas Sousa, coordenador de Relações Governamentais do Saúde Digital Brasil (SDB).

"A interoperabilidade, ao mesmo tempo que é extremamente necessária, é difícil, porque envolve reunir dados de todos os cidadãos, de consultórios médicos, prestadores de serviços públicos e privados e, diante disso, ainda é preciso enfrentar questões relacionadas à privacidade de dados. As dificuldades tecnológicas são as menores. Temos questões importantes a enfrentar, como financeiras, operacionais e jurídicas", analisa Antônio Britto, diretor-executivo da Associação Nacional de Hospitais Privados (Anahp).

Os países europeus têm investido em projetos de Tecnologias de Informação e Comunicação em Saúde (eHealth) para reduzir custos e centralizar o paciente no sistema. "A Itália economiza 1 euro para cada 9 gastos em procedimentos médicos devido ao eHealth. Na Holanda, Dinamarca e Reino Unido, mais de 80% dos atendimentos utilizam o Registro Eletrônico do Paciente. Estônia, Croácia e Suécia fazem mais de 95% de suas prescrições médicas eletronicamente. Essa tendência também é observada na América do Norte, Ásia, Oceania, partes da América do Sul e alguns países africanos", destaca Sousa.

3. Benckmarck / Boas Práticas

3.1. Interoperabilidade de dados na saúde

Desde a instituição do SUS na Constituição Federal de 1988, a saúde se tornou um direito fundamental e objeto de políticas públicas para a cobertura de saúde em todo território nacional. Com a publicação em 2004 da Política Nacional de Informação e Informática em Saúde (PNIIS), o Ministério da Saúde desenvolveu estratégias para transformação digital, informatização da saúde pública e interoperabilidade desses dados coletados.

Segundo o site do Departamento de Informática do SUS, o DATASUS, a interoperabilidade tem[9] "o objetivo é promover a utilização de uma arquitetura da informação em saúde que contemple a representação de conceitos para permitir o compartilhamento de dados em saúde, além da cooperação de todos profissionais, estabelecimentos de saúde e demais envolvidos na atenção à saúde prestada ao usuário do SUS, em meio seguro e com respeito ao direito de privacidade".

O conceito de interoperabilidade pode ser definido como *"a capacidade dos sistemas, unidades, ou forças de disponibilizarem serviços para, e aceitarem serviços de outros sistemas, unidades, ou forças e de utilizarem estes serviços no sentido de operarem eficazmente em conjunto"*[10]. Observa-se que há, portanto, uma integração de elementos, sistemas e pessoas trabalhando em conjunto.

De uma forma simples, interoperabilidade constitui a capacidade de pessoas, instituições e sistemas interagirem para que de forma eficiente e eficaz possam trocar e utilizar informação, visando a contribuir para um fim comum[11].

A interoperabilidade no setor de saúde refere-se à capacidade de diferentes sistemas de informação, como prontuários eletrônicos, plataformas de telemedicina, laboratórios e sistemas hospitalares, comunicarem entre si e trocarem dados de maneira eficiente. A interoperabilidade permite que o histórico médico de um paciente, exames, diagnósticos, tratamentos e outras informações relevantes sejam acessíveis a qualquer instituição autorizada, independentemente do sistema que utilizam.

Essa interoperabilidade traz uma gama de benefícios para o sistema de saúde brasileiro:

[9] https://datasus.saude.gov.br/catalogo-de-servicos/
[10] DoD JP1-02, Department of Defense Dictionary of Military and Associated Terms (As Amended Through 15 August 2012), vol. 2010, no. November 2010. Joint Publication 1-02, 2010.
[11] S. A. Baird, "Government Role in Developing an Interoperability Ecosystem," ICEGOV2007, December 10-13, 2007, Macao, pp. 65–68, 2007

- **Melhoria na continuidade do cuidado:** Com dados clínicos acessíveis de forma instantânea, os profissionais de saúde conseguem oferecer um tratamento mais eficiente, evitando a duplicação de exames e otimizando o tempo de resposta a emergências.
- **Tomada de decisão baseada em dados:** O acesso a informações completas e atualizadas do paciente facilita decisões clínicas mais precisas, o que melhora os resultados do tratamento.
- **Facilitação da mobilidade de pacientes:** Em um país de grandes dimensões como o Brasil, pacientes muitas vezes precisam de atendimento em diferentes localidades. A interoperabilidade permite que o histórico de saúde do paciente seja facilmente acessado por profissionais de saúde em qualquer ponto do território nacional.
- **Capacitação do paciente:** A interoperabilidade permite que os pacientes tenham acesso ao seu próprio histórico de saúde de forma transparente, promovendo uma maior participação e responsabilidade nos cuidados de saúde.
- **Melhoria na investigação e saúde pública:** A agregação de dados de forma anônima pode ajudar na análise de tendências de saúde, no desenvolvimento de novos tratamentos e na monitorização de surtos de doenças.
- **Integração entre o público e o privado:** O Brasil possui um sistema de saúde misto, e a interoperabilidade é essencial para garantir que as informações fluam entre os sistemas de saúde pública e privada.

Em 2020, o Ministério da Saúde, através do DATASUS, publicou a Portaria GM/MS nº 1.434, de 28 de maio de 202012, instituindo a Rede Nacional de Dados em Saúde (RNDS), plataforma nacional de interoperabilidade (troca de dados) em saúde. Além de ser um projeto estruturante do Conecte SUS, a RNDS é um programa do Governo Federal voltado para a transformação digital da saúde no Brasil e tem o objetivo de promover a troca de informações entre os pontos da Rede de Atenção à Saúde, permitindo a transição e continuidade do cuidado nos setores públicos e privados.

[12] https://www.in.gov.br/en/web/dou/-/portaria-n-1.434-de-28-de-maio-de-2020-259143327

O programa é voltado à informatização da atenção à saúde e à integração dos estabelecimentos de saúde públicos e privados e dos órgãos de gestão em saúde dos entes federativos, para garantir o acesso à informação em saúde necessário à continuidade do cuidado do cidadão.

A Portaria de Consolidação nº 1/GM/MS, de 28 de setembro de 2017, que dispõe sobre a Consolidação das normas sobre os direitos e deveres dos usuários da saúde, a organização e o funcionamento do Sistema Único de Saúde, estabelece no seu art. 236 que "os Municípios, os Estados e o Distrito Federal podem optar pela utilização de padrões de interoperabilidade distintos ou complementares àqueles definidos pelo Ministério da Saúde, desde que seja garantida a interoperabilidade com os padrões nacionais."13. Esse artigo possibilitou, portanto, que os entes federativos desenvolvessem modos de tornar os dados dentro da sua unidade administrativa interoperáveis, como é o caso do município do Rio de Janeiro.

No entanto, à medida que a interoperabilidade cresce, o volume de dados sensíveis que circula entre sistemas aumenta significativamente, levantando questões sérias sobre a privacidade e a proteção dessas informações.

3.2. Privacidade e Proteção de Dados na Interoperabilidade

Sem a pretensão de entrar na problemática sobre as técnicas de interoperabilidade de sistemas e como se dão as etapas da integração dos mesmos, nos propomos a analisar a interoperabilidade sob o viés da privacidade e proteção dos dados pessoais compartilhados.

Como foco do estudo em questão são os dados de saúde em um sistema interoperável, a própria natureza desses dados torna a privacidade um aspecto crítico, que vai permear todo processo de integração, estruturação e responsabilização dos usuários do banco de dados criado.

O avanço da ampliação do acesso à saúde pelo Sistema Único de Saúde (SUS) também é fruto dos avanços tecnológicos na prestação de serviços de saúde. Desta forma, a digitalização de prontuários médicos, exames clínicos e laboratoriais, assim como a integração com outras áreas, farmacológica e de terapias que integram a promoção à saúde produziram grandes bancos de dados de saúde.

[13] https://bvsms.saude.gov.br/bvs/saudelegis/gm/2017/MatrizesConsolidacao/Matriz-1-SUS.html

Porém, não havia nenhum tipo de conexão entre esses bancos de dados de saúde criados e, portanto, não poderiam, sozinhos, promover uma visão geral da saúde do paciente, possibilitando uma melhor prestação de serviços de saúde integral, diagnósticos mais completos e medidas de prevenção à saúde do paciente, como determinado pela estratégia do desenvolvimento da Atenção Primária em Saúde.

Porém, com o advento das leis de proteção à privacidade e proteção de dados, essa evolução e interoperabilidade de sistemas tem que ser pensada à luz da proteção de dados pessoais do titular desde a sua concepção. É necessário garantir que os dados serão transmitidos de forma segura e só acessíveis a pessoas autorizadas e que tenham tido formação profissional para sua correta utilização, bem como que contenham trilha de auditoria, de modo a não serem extraídos de forma oculta dos sistemas.

Ademais, a intensificação na digitalização e integração de dados, por exemplo, com a instalação dos prontuários médicos eletrônicos e sistemas interoperáveis, aumenta a vulnerabilidade a ciberataques[14], podendo interromper a prestação da assistência e expor informações sensíveis de pacientes.

Para mitigar esses riscos, as instituições de saúde devem adotar medidas rigorosas de cibersegurança, como a criptografia de dados, autenticação multifator, métodos de resiliência, como política de continuidade de operações, e a atualização regular dos sistemas, visto que a partilha de dados entre diferentes sistemas e instituições pode criar lacunas de segurança, especialmente se esses sistemas não forem adequadamente protegidos[15].

Em outro viés de segurança, é necessário investir em educação e formação de profissionais de saúde e funcionários administrativos que lidam com dados sensíveis. A formação deverá garantir que as políticas de proteção de dados sejam corretamente seguidas. Muitas violações de privacidade resultam de erros humanos, como o envio de

[14] https://www.darkreading.com/cyberattacks-data-breaches/synnovis-ransomware-attack-disrupts-operations-london-hospitals
- https://www.darkreading.com/cyber-risk/healthcare-providers-and-hospitals-under-ransomware-s-siege
-https://www.darkreading.com/cyberattacks-data-breaches/south-africa-healthcare-lab-still-reeling-from-ransomware-attack
-https://www.darkreading.com/cyberattacks-data-breaches/novant-health-notifies-patients-of-potential-data-privacy-incident
-https://www.darkreading.com/cyberattacks-data-breaches/nhs-breach-hse-bug-expose-healthcare-data-british-isles

[15] Belli et al. (2024) apresentam mapeamento normativo relativo à cibersegurança no setor público brasileiro, indicando boas práticas e requisitos normativos nas esferas federal e estadual. Belli et al. (2023) também apresentam boas práticas baseadas em análise mais ampla de práticas de mercado, bem como tipos mais comuns de vulnerabilidades cibernéticas.

informações para o destinatário errado ou o uso de senhas fracas ou fora do padrão estabelecido nas políticas de controle de acesso.

Em um futuro próximo será também possível aproveitar a interoperabilidade de sistemas para utilização de tecnologias com inteligência artificial e os chamados *wearables*[16]. Garantir que nas primeiras etapas sejam respeitadas a privacidade e proteção de dados dos titulares é mais que necessário para se preparar para que os novos desafios já tenham uma base forte de proteção e mitigação de riscos.

4. Recomendações

Na interoperabilidade referente à oferta de dados pessoais e sensíveis dos pacientes nos diversos locais deverá haver uma infraestrutura tecnológica que possibilite conectar todos os envolvidos no atendimento do sistema de saúde, como médicos, dentistas, psicoterapeutas, hospitais, farmácias e demais usuários, na medida de privilégio de acesso baseado na necessidade de saber (“need to know basis”).

Caberá à Secretaria Municipal de Saúde criar metodologias através de pesquisa histórica e estatística na realização de regulamentos e normativos internos de segurança da informação dos usuários da saúde, assim como na movimentação desses dados pelos agentes de saúde, médicos e demais envolvidos no processo.

Nesse processo deverão ser programadas ações de curto, médio e longo prazo. Essas ações deverão contemplar normativo legal ou administrativo:

- Na busca de saúde física e mental, através de programas de orientação à população nos dados pessoais e sensíveis coletados, a fim de garantir sua responsabilidade constitucional;
- Proteção extra na execução de medidas de urgência, emergência e atendimento domiciliar, a fim de garantir a privacidade dos dados pessoais e sensíveis;
- Aperfeiçoamento do administrador hospitalar e da sua equipe quanto a à proteção de dados pessoais e sensíveis dos seus administrados;

[16] Todo e qualquer dispositivo tecnológico que possa ser usado como acessório ou que podemos vestir é um *wearable*. Afinal, essa é a tradução do termo inglês. Dentre eles, os mais populares atualmente são os *smartwatches* e *smartbands*, dispositivos que têm o monitoramento da saúde como seus principais recursos

Ainda, em consonância com a proposição da implantação de um ambiente de interconectividade em saúde pelo Ministério da Saúde, entendemos que a interoperabilidade deverá se dar em níveis de desenvolvimento, com resultados progressivos, acumulando aprendizados para as próximas etapas.

Em um primeiro momento, se faria a integração dos sistemas de saúde de atenção primária, através de interoperabilidade dos sistemas de prontuário eletrônico, em vistas de ser atenção primária elemento fundamental, ordenador do cuidado.

Posteriormente, essa integração se daria com a rede de atenção hospitalar de urgência e emergência, através de seus prontuários médicos eletrônicos. Formar-se-ia, assim, um histórico clínico integrado do paciente, funcionando para consultas e análise preliminar para a prestação do cuidado de saúde, tendo uma visão geral do histórico do paciente, visando uma melhor prestação do serviço público de saúde.

Um terceiro passo seria integrar laboratórios públicos ao Histórico Clínico Integrado (HCI) do paciente, viabilizando a análise de todos os profissionais em cadeia de atendimento ao paciente, tanto na estrutura da atenção primária, quanto na estrutura de urgência e emergência. A disponibilização dos resultados ajudaria na prestação do atendimento e acabaria com a duplicidade de pedidos de um mesmo exame ou mesmo a demora na análise por profissionais de saúde.

Outra etapa seria a integração com a rede de farmácias dos SUS, indicando o histórico de uso de medicamentos do paciente pela dispensação na rede, encerrando, assim, a primeira etapa de integração em sede municipal. As etapas posteriores seriam a interoperabilidade com os sistemas estaduais e federais.

Destacamos também a necessidade falar de divulgação/intercâmbio das iniciativas em fóruns nacionais, para permitir um direcionamento conjunto desde a fase de concepção, evitando que cada ente siga caminhos diferentes, como ocorre atualmente com a não-integração do CNAE nacional e o fluminense, que prejudica o gozo da lei de liberdade econômica.

Concluídas todas as etapas na administração pública, haveria o início da integração com os sistemas de saúde suplementar e privados. Porém, essa etapa só seria viabilizada com as medidas e salvaguardas necessárias e aprendidas com a integração dentro dos sistemas públicos.

Importante ressaltar a necessidade de adoção e definição de padrões para integração dos sistemas, armazenamento do banco de dados criado pelo HCI, além da

observância dos aspectos legais referentes ao uso dessas informações, garantindo a privacidade dos pacientes e a proteção dos dados sensíveis de saúde.

Esses padrões, além de viabilizar a interoperabilidade dos sistemas, da segurança jurídica e segurança da informação, possibilitarão novas funcionalidades e aplicações para a melhora contínua da prestação de serviços em saúde e execução de políticas públicas.

Porém, é importante ressaltar que quanto maior o nível de interoperabilidade de sistemas, maior será o número de pessoas autorizadas a utilizar esse banco de dados e, assim, acessar dados pessoais e dados pessoais sensíveis que foram compartilhados.

Desta forma, serão também recomendados por esse Relatório requisitos básicos para boas práticas no desenvolvimento de todo projeto de interoperabilidade de dados:

1. Minimização de dados: Somente aqueles dados de saúde que são necessários para o respectivo propósito podem ser coletados e processados. Informações desnecessárias ou supérfluas devem ser evitadas;
2. Limitação de finalidade: Dados de saúde podem ser processados somente para as finalidades para as quais foram coletados. O uso para outras finalidades é permitido somente em casos excepcionais e sob certas condições.
3. Segurança de dados: Medidas técnicas e organizacionais apropriadas devem ser tomadas para garantir a segurança dos dados de saúde. Isso inclui medidas como criptografia, controles de acesso e verificações de segurança regulares.
4. Processamento terceirizado: se os provedores de serviços processarem dados pessoais em nome dos controladores destes dados (por exemplo, provedores de serviços de TI), eles devem respeitar o contrato de prestação de serviços celebrado, com cláusulas claras e rígidas de confidencialidade e responsabilidade na proteção de dados pessoais e sensíveis dos pacientes;
5. Direitos dos titulares dos dados: Os pacientes têm o direito à informação sobre seus dados armazenados, o direito à retificação de dados

imprecisos, o direito à exclusão sob certas condições e o direito à portabilidade dos dados, se for o caso.

6. Em se tratando de interoperabilidade de prontuários médicos e informações de saúde do paciente, como é o caso do HCI da SMS-Rio, os pacientes deverão ter acesso ao seu HCI quando todas as integrações tiverem sido finalizadas e ter disponível para sua ciência todo o histórico de usuários que acessaram o seu HCI, garantindo assim, a transparência legal;
7. Notificação de violação de proteção de dados: No caso de violações de dados que representem um risco aos direitos e liberdades dos titulares dos dados, deverá haver uma comunicação pública e informação clara sobre o ocorrido a ANPD, nos termos da resolução CD/ANPD nº 15/2024;
8. Avaliação de impacto na proteção de dados: A Secretaria Municipal de Saúde (SMS-Rio) deverá analisar a pertinência de elaboração de um relatório de impacto de dados pessoais quanto ao processamento de dados de saúde em ambientes de interoperabilidade, avaliando se representa um alto risco para os direitos e liberdades dos titulares dos dados. A integração de sistemas deverá estar condicionada à realização deste relatório, que deverá justificar a sua adequação e necessidade tendo em vista os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
9. Em casos de incidentes de segurança de dados pessoais e sensíveis deverá haver um plano de restabelecimento dos serviços, assim como documentação e avaliação sobre as falhas e vulnerabilidades ocorridas e medidas adotadas em resposta. Ademais, deverá haver um plano de contingência para retomada das atividades parcial ou total dos serviços aos pacientes;
10. Nos hospitais de médio e grande porte, sob a responsabilidade da Secretaria Municipal de Saúde, deverá haver uma sala de back-up local a fim de garantir a continuidade dos atendimentos, principalmente emergenciais, devido à sua sensibilidade no resultado.

Recomendações quanto à estrutura tecnológica:

A Secretaria Municipal de Saúde deverá contar com provedores de serviços tecnológicos em sua estrutura organizacional. Se houver terceirização do tratamento de dados, seja por serviços de desenvolvimento ou serviços de nuvem, deverá haver cláusula rígida de Privacy by Design e Privacy by Default dos sistemas de serviços de saúde. Ademais, deverá haver termos de responsabilidade para os atendentes, enfermeiros, médicos, laboratórios de diagnóstico e demais usuários do sistema.

Recomendações ao Encarregado de Proteção de Dados

A tarefa do Encarregado pela proteção de dados é de extrema importância, pois buscará aconselhar quanto à execução dos princípios mínimos de proteção de dados pessoais e sensíveis, seu tratamento e seu armazenamento, inclusive propondo normas de governança que prevejam sua participação desde o desenvolvimento do projeto, para viabilizar o *privacy by design*.

Numa possível violação caberá a ele a análise, junto ao Comitê de Privacidade e Proteção de Dados Pessoais e a Encarregada Geral de Dados da Prefeitura do Rio de Janeiro, e a posterior divulgação pública do ocorrido, bem como a comunicação à ANPD. A extensão de sua atuação abrange todas as unidades da área de Saúde no âmbito do município do Rio de Janeiro, desde a Clínica da Família, passando pelos centros de atendimento médico conveniado até os grandes hospitais municipais. A extensão é enorme: mais de 400 unidades de saúde entre Clínicas da Família, Centros Municipais de Saúde, Centros de Urgência e Emergência, Hospitais Especializados, cabendo à Secretaria Municipal de Saúde (SMS-Rio) a criação de estrutura, no âmbito de sua organização administrativa, que possua recursos humanos e tecnológicos para dar suporte à atuação do Encarregado. Essa estrutura seria responsável pela avaliação de impacto, monitoramento dos ambientes de execução, acompanhamento do sistema do SUS, proteção e resposta sob um possível ataque malicioso nos dados pessoais e sensíveis sob sua responsabilidade.

5. Conclusão

A política de transformação digital na saúde pública apresenta diversos riscos, muitos deles inerentes ao tratamento de dados em plataformas unificadas e

interoperáveis – especialmente aquelas que lidam com grandes volumes de dados pessoais. Esses sistemas deverão estar alinhados com as leis de proteção de dados e privacidade e serem objeto de controles contínuos, como o monitoramento regular e processos constantes de atualização tecnológica. A interoperabilidade de dados na saúde oferece grandes oportunidades para aprimorar a continuidade e a qualidade dos serviços públicos, especialmente no Sistema Único de Saúde (SUS). É imprescindível equilibrar os benefícios da integração com as salvaguardas de segurança, garantindo transparência, responsabilidade e cumprimento dos direitos dos cidadãos. A criação de uma cultura de segurança da informação será vital para que a interoperabilidade contribua efetivamente para um sistema de saúde digital e ético.

Esse Relatório trouxe medidas e salvaguardas para que o ambiente de interoperabilidade de dados na saúde dentro da Prefeitura do Rio de Janeiro, seja construído respeitando a privacidade e proteção de dados pessoais dos titulares e ainda, com medidas robustas de segurança da informação.

Assinaturas dos membros do GT

1- Alessandra Almeida Lapa
2- Carlos Alexandre
3- Fernando Bourguy
4- Horrara Moreira
5- Walter Gaspar
6- Rafael Barboza
7- Vitor Paludetto