

# **Estudo: Compartilhamento de dados de saúde**

Dr. Juliano Maranhão  
Dr. Ricardo Campos

## Juliano Maranhão



Bacharel, doutor e livre docente pela Faculdade de Direito da Universidade de São Paulo, onde é professor do Departamento de Filosofia e Teoria Geral do Direito. Pesquisador da Fundação Alexander von Humboldt e professor convidado da Goethe Universität Frankfurt am Main (Alemanha). Pós-doutorado na faculdade de ciência da computação da Universidade de Utrecht (Holanda). Membro do Comitê Diretor da International Association for Artificial Intelligence and Law (IAAIL). Diretor do Instituto Legal Grounds. Sócio do Opice Blum, Bruno e Vainzof.

## Ricardo Campos



Docente na faculdade de direito da Goethe Universität Frankfurt am Main (Alemanha). Mestre e Doutor pela Goethe Universität. Especializado em regulação de serviços digitais, proteção de dados, direito público e regulatório. Ganhador do renomado prêmio Werner Pünder (2021) sobre regulação de serviços digitais. Atua no Brasil como consultor em processo legislativo em temas do direito digital e digitalização. Coordenador da área de Direito Digital da OAB Federal/ESA Nacional. Diretor do Instituto Legal Grounds (Sao Paulo). Sócio do Opice Blum, Bruno e Vainzof.



# Sumário Executivo

Cada vez mais, o processamento computacional de dados de saúde de pacientes tem apoiado a tomada de decisões clínicas, permitido o planejamento, supervisão e melhoria do sistema de saúde e fornecido informações para capacitar os pacientes a se engajarem ativamente em sua gestão de saúde e bem-estar. Dentre os dados mais relevantes para assistir o médico no tratamento do paciente, bem como fornecer insumos para análises abrangentes sobre o funcionamento dos sistemas de saúde de maneira geral, estão aqueles obtidos diretamente do paciente durante a realização de procedimentos anteriores por profissionais de saúde, em clínicas, hospitais e outros estabelecimentos prestadores de serviços de saúde, que formam os *prontuários médicos*.

Essa integração somente é possível na medida em que os diferentes sistemas informáticos nos quais são armazenados os prontuários eletrônicos, nas diferentes unidades de atendimento, sejam interoperáveis. Definida de modo geral, a interoperabilidade é a capacidade de um sistema ou produto informático de funcionar com outros sistemas ou produtos sem que se demande esforços especiais por parte do usuário. A *informatização dos prontuários e a interoperabilidade dos níveis de atendimento à saúde*, objetos de análise deste estudo, é uma tendência global, que se vê desenvolvida no Brasil com a Estratégia de Saúde Digital para o Brasil 2020-2028, do Ministério da Saúde.

O ponto é que, em um contexto de incentivo à digitalização de prontuários e a interoperabilidade de sistemas de atenção, reforça-se a coleta, tratamento e compartilhamento de dados pessoais de natureza sensível. Isso pode trazer uma série de implicações referente aos direitos dos titulares de dados, dispostos tanto na Constituição Federal quanto em legislações infraconstitucionais, cujo principal exemplo em nosso ordenamento é a Lei Geral de Proteção de Dados Pessoais (LGPD), de 2018. Não por outro motivo, a proteção de dados pessoais é uma das principais preocupações na implementação de um sistema de e-saúde (*e-health*) centrada no paciente e capaz de assegurar seus direitos fundamentais. No Brasil, há diferentes iniciativas no sentido de desenvolvimento de sistemas de *e-health*, baseadas no tratamento de dados de saúde a partir de prontuários eletrônicos, sendo necessário questionar em que medida são compatíveis com o regime de proteção de dados estabelecido no país e também internacionalmente.

Uma dessas iniciativas, que comporá o foco central deste estudo, está na requisição, por algumas Operadoras de Planos de Saúde (OPS), de compartilhamento do prontuário eletrônico, como condição para o cadastro de hospitais e clínicas que pretendam fazer parte da rede de estabelecimentos de saúde credenciados. Tal requisição é feita com base em uma série de argumentos, que serão destrinchados nas páginas seguintes. Nesse sentido, os questionamentos que orientam o estudo apresentado podem ser resumidos da seguinte maneira: as Operadoras de Planos de Saúde (OPS) teriam direito ao acesso aos dados de saúde constantes no prontuário médico sem o consentimento do paciente/ usuário do serviço de saúde, com base nos Art. 7º, VIII e Art. 11, II, "f", da LGPD?

Para o exame da compatibilidade da requisição de prontuários médicos por operadoras de saúde com o direito à proteção de dados pessoais, partimos inicialmente de uma análise comparada, estudando a experiência internacional em relação à implementação de projetos de *e-health* baseados na interoperabilidade de prontuários eletrônicos. Analisam-se as disposições gerais aplicáveis à União Europeia, sobretudo a partir do Regulamento Geral sobre Proteção de Dados Pessoais (GDPR), bem como as legislações de países específicos, nomeadamente Alemanha, Espanha, França e Itália. São analisados ainda os regimes da Inglaterra, Estados Unidos da América e Argentina.

Em um segundo momento, o estudo volta-se à análise pormenorizada do regime de proteção de dados pessoais no Brasil, com foco no compartilhamento de dados pessoais de saúde. A partir de uma abordagem legal e jurídica, as normas sobre proteção de dados pessoais no país são analisadas de maneira abrangente, envolvendo desde o estudo do direito fundamental à proteção de dados pessoais, manifestado, no caso em questão, como direito à autonomia informacional, até a análise legal e de normativas, resoluções e pareceres.

Em apertada síntese, as principais conclusões do estudo são:

- 1) A interoperabilidade do sistema de saúde via seguradoras privadas de saúde não foi observada de maneira compulsória nos diferentes ordenamentos jurídicos analisados, sendo cabível somente mediante consentimento do titular, que deve ser livre, informado, inequívoco, específico e destacado;
- 2) No Brasil, são duas as bases legais que legitimam o compartilhamento de dados de saúde com OPSs: o cumprimento de obrigação legal ou regulatória pelo controlador e o consentimento do titular;

- 3) A hipótese de cumprimento de obrigação legal ou regulatória pelo controlador limita as informações a serem compartilhadas entre hospitais e seguradoras de saúde ao estritamente necessário para: verificação de elegibilidade; autorização de procedimentos; comunicação de internação ou alta do beneficiário; cobrança de serviços de saúde; demonstrativos de retorno; envio e recebimento de documentos necessários para solicitação, autorização e cobrança; recurso de glosa; comprovante presencial;
- 4) No caso de consentimento pelo titular, este deve ser expresso, informado, inequívoco e em cláusula separada do contrato de prestação de serviços ou em instrumento próprio (nos termos do art. 8º e art. 11 da LGPD);
- 5) Não se legitima o tratamento de dados pessoais, em particular o acesso a prontuários médicos, por seguradoras de saúde, com base na alínea f, inc. II, do art. 11 da LGPD. Isso porque seguradoras de saúde não constituem prestadoras de serviços de saúde, mas apenas intermediadoras de serviços de saúde prestados por terceiros (médicos e estabelecimentos de saúde);
- 6) Com relação ao projeto de prontuário médico único, que centralizaria os dados de prontuários médicos de estabelecimentos de saúde públicos e privados nas mãos do Estado, o presente estudo aponta que a experiência internacional, com exceção da Inglaterra, segue a tendência oposta, no sentido de promover a interoperabilidade no acesso a dados por meio de padronização técnica e semântica, não de centralização da base de dados. Além disso, o estudo vislumbra óbices constitucionais, tendo em vista o princípio de separação de poderes informacional, corolário do direito fundamental à proteção de dados, bem como aponta riscos quanto à unidade informacional, em particular quanto ao impacto mais grave em incidentes de segurança e vazamento de dados.

---

---

# Sumário

Introdução: medicina digital, prontuários eletrônicos e interoperabilidade .....	9
2. Experiência internacional em e-health, interoperabilidade de prontuários médicos e compartilhamento de dados com seguradoras .....	15
2.1. Europa .....	15
2.1.1 Usos primários .....	17
2.1.2 Usos secundários .....	18
2.2. França .....	20
2.2.1 Organização do sistema de saúde francês .....	22
2.2.2 O sistema francês de dados de saúde .....	20
2.2.3 “Mon Espace Santé” .....	21
2.2.4 Interoperabilidade no sistema de saúde francês.....	22
2.2.5 Seguro saúde e dados pessoais na França.....	23
2.3 Espanha .....	25
2.3.1 Organização do sistema de saúde espanhol.....	25
2.3.2 O sistema nacional de dados de saúde espanhol.....	26
2.3.3 Interoperabilidade no sistema de saúde espanhol.....	28
2.3.4 Seguro Saúde e dados pessoais na Espanha .....	29
2.4 Alemanha.....	31
2.4.1 Organização do sistema de saúde alemão.....	31
2.4.2 O uso de dados de saúde na Alemanha .....	33
2.4.3 Digitalização e Interoperabilidade de dados de saúde na Alemanha.....	36
2.5 Itália.....	42
2.5.1 Organização do sistema de saúde italiano .....	42
2.5.2 O sistema italiano de dados de saúde .....	43
2.5.3 Seguro saúde e dados pessoais na Itália.....	45
2.6 Conclusões parciais sobre países da Comunidade Europeia .....	46
2.7 Inglaterra.....	48

2.7.1 O sistema de saúde inglês.....	48
2.7.2 Proteção de dados de saúde na Inglaterra .....	49
2.7.3 Saúde digital no Reino Unido e interoperabilidade .....	52
2.7.4 Conclusões parciais sobre o sistema inglês.....	56
2.8 Estados Unidos da América.....	57
2.8.1 O sistema de saúde dos EUA .....	57
2.8.2 O uso de dados pessoais no setor de saúde dos EUA .....	58
2.8.3 Saúde digital e interoperabilidade nos EUA .....	61
2.8.4 Compartilhamento com seguradoras e preocupações em relação a empresas de TI	66
2.8.5 Conclusões parciais sobre o sistema estadunidense.....	68
2.9 Argentina .....	69
2.9.1 O Sistema de Saúde na Argentina .....	69
2.9.2 Proteção da saúde e dos dados pessoais - Privacidade dos dados.....	70
2.9.3 O Sistema Nacional de Dados de Saúde: Registros médicos e a interoperabilidade dos dados médicos na Argentina .....	71
2.9.4 Compartilhamento de registros médicos com seguradoras de saúde.....	73
2.9.5 Conclusões parciais sobre o sistema argentino.....	75
3.Compartilhamento de dados de saúde no Brasil.....	78
3.1. Modelo de assistência à saúde no Brasil.....	78
3.2 Compartilhamento de informações de saúde na saúde suplementar .....	84
3.2.1 A Coleta de Dados de Saúde e a gestão de pagamento na saúde suplementar	84
3.3 Bases legais para o compartilhamento de dados de saúde entre estabelecimentos de saúde e Operadoras de Planos de Saúde conforme a Lei Geral de Proteção de Dados.....	91
3.3.1 Bases Legais autorizadoras de tratamento conforme a LGPD .....	91
3.3.2 Possíveis bases legais para o compartilhamento de dados entre estabelecimentos de saúde e OPSs.....	94
3.3.3 Conceito de serviço de saúde .....	97
3.3.4 Direito comparado e a Regulamentação do Programa Conecte SUS.....	102
3.4.5 Considerações sobre a implantação de interoperabilidade e o acesso a prontuários eletrônicos no Brasil .....	103
4.Potenciais problemas concorrenciais derivados do compartilhamento de dados sensíveis de saúde às operadoras de planos de saúde .....	108
5.Considerações finais.....	115



# Introdução: medicina digital, prontuários eletrônicos e interoperabilidade

O uso de tecnologias digitais tem transformado o setor de saúde, com a ampliação do conhecimento, a criação de novos métodos de diagnóstico e tratamento.<sup>1</sup> O uso de tecnologias digitais tem transformado o setor de saúde, com a ampliação do conhecimento, a criação de novos métodos de diagnóstico e tratamento. Esses avanços baseados na digitalização somente concretizam sistemas de saúde seguros, eficientes e sustentáveis na medida em que o processamento de dados sobre os pacientes e sobre a população possuam respaldo legal e segurança jurídica. Esses dados hoje se encontram, sobretudo, nos prontuários eletrônicos.

Assim, o processamento computacional desses dados é capaz de apoiar a tomada de decisões clínicas, permitir o planejamento, supervisão e melhoria do sistema de saúde e podem fornecer informações para capacitar os pacientes a se engajarem ativamente em sua gestão de saúde e bem-estar.<sup>2</sup> Tal processamento inclui dados formalmente estrutura-

---

1 Expert Panel on effective ways of investing in Health (EXPH) (2019) Assessing the Impact of Digital Transformation of Health Services. Luxembourg: Publications Office of the European Union.

2 European Commission (2018) Commission Staff Working Document Accompanying the Document Communication from the Commission to the European Parliament, the Council, the European

dos em registros eletrônicos de saúde, imagens médicas, prescrições de medicamentos, relatórios laboratoriais, reclamações e dados de reembolso, resultados relatados pelos pacientes e outras ferramentas de gerenciamento de dados usadas dentro dos sistemas de saúde. Pode incluir também dados gerados fora do ambiente de saúde, tais como dados de dispositivos de bem-estar, tais como rastreadores de fitness e outros dados provenientes de uma ampla gama de ambientes.

Dentre os dados mais relevantes para assistir o médico no tratamento de doenças estão aqueles obtidos diretamente do paciente durante a realização de procedimentos anteriores por profissionais de saúde, em clínicas, hospitais e outros estabelecimentos prestadores de serviços de saúde, que formam os *prontuários médicos*.

O prontuário médico é documento essencial em qualquer acompanhamento de um paciente e se tornou obrigatório em todo o Brasil a partir de 1988.<sup>3</sup> Conforme determina a Resolução 1.638 do Conselho Federal de Medicina (“CFM”), o prontuário é um “*documento único constituído de um conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo.*” Assim, o prontuário se pretende totalizante, englobando todas as informações relevantes disponíveis para assistir a decisão da equipe médica que realiza os cuidados do paciente.

Os prontuários se mantêm registrados no ponto de atendimento de saúde de forma perene. Isto é, as informações de prontuário havidas numa visita hospitalar anos atrás continuarão constando no prontuário do paciente, que é alimentado com novas informações a cada visita realizada. Assim, eles refletem as informações colhidas em um *locus* específico, um hospital, uma clínica médica etc., de maneira que, ainda que sejam mantidos todos os registros, o histórico do paciente dificilmente se reflete integralmente em um único prontuário. A ida a outro ponto de atendimento de saúde gerará um novo prontuário, com informações paralelas àquelas do prontuário de outra unidade de saúde.

Prontuários são realizados em suportes físicos (papel) ou em formato eletrônico. O Brasil regulou o uso de prontuários eletrônicos a partir de 2002,<sup>4</sup> e passou a determinar parâmetros mínimos de segurança<sup>5</sup> nos anos seguintes. Isto favorece a adoção da versão digital dos prontuários, mas os recursos necessários a este movimento nem sempre estão disponíveis a todos os pontos de atendimento de saúde e, particularmente, estão pouco disponíveis na rede pública apesar do crescimento na implementação de recursos digitais nos últimos anos.<sup>6</sup>

Dentre informações pessoais presentes nos prontuários estão anamnese, consultas, anotações do médico sobre a consulta, diagnósticos de doença, exames, resultados de

Economic and Social Committee and the Committee of the Regions on Enabling the Digital Transformation of Health and Care in the Digital Single Market. Brussels: SWD, 126 final.

3 Código de Ética Médica, 1988. Art. 69.

4 Resolução 1.639/2002 do CFM.

5 1.821/2007 CFM; 2.218/2018.

6 ICT in Health Survey 2021

[https://cetic.br/media/docs/publicacoes/2/20211124124340/executive\\_summary\\_ict\\_health\\_survey\\_2021.pdf](https://cetic.br/media/docs/publicacoes/2/20211124124340/executive_summary_ict_health_survey_2021.pdf)

exames, procedimentos médicos, medicamentos administrados, internações e dados relacionados ao seu atendimento assistencial, *check up* etc. No caso de prontuários eletrônicos, também é possível acessar metadados sobre horário, identidade e local dos acessos realizados por médicos ou profissionais de saúde ao prontuário.

Em termos de gestão do atendimento à saúde, o prontuário eletrônico tem o potencial de concretizar o *desideratum* de um sistema *centrado no paciente*,<sup>7</sup> na medida em que pode ser integrado em plataformas de tecnologia da informação que acompanhem o paciente em todo o ciclo de atendimento, incluindo hospitalização, visitas ambulatoriais, exames, testes, fisioterapia etc., em diferentes unidades de atendimento, de modo que os dados são agregados tendo em vista as necessidades dos pacientes e não dos prestadores de serviços de saúde.

Essa integração somente é possível na medida em que os diferentes sistemas informáticos nos quais são armazenados os prontuários eletrônicos, nas diferentes unidades de atendimento, sejam interoperáveis. Definida de modo geral, a interoperabilidade é a capacidade de um sistema ou produto informático de funcionar com outros sistemas ou produtos sem que se demande esforços especiais por parte do usuário.<sup>8</sup> Ou seja, a interoperabilidade não se limita à troca de informações entre sistemas, mas inclui a possibilidade de o sistema receptor executar funções, a partir dos inputs recebidos do outro sistema. Ela abrange distintas camadas, a técnica, a semântica e a organizacional. A interoperabilidade técnica permite a troca de dados de um sistema a outro. A interoperabilidade semântica exige que o dado obtido pelo receptor seja compreendido no mesmo sentido, sem ambiguidades, daquele usado no sistema emissor. Para tanto, deve haver alguma uniformidade nos conceitos empregados por ambos os sistemas. A interoperabilidade organizacional pressupõe o alinhamento dos processos e gestão entre as duas organizações que controlam os sistemas operacionais.

Há diferentes tipos de interoperabilidade que podem ser alcançados pela integração de sistemas: a) *Interoperabilidade de Protocolo* relacionada à interoperabilidade entre serviços complementares (exemplo: duas clínicas distintas conseguem acessar o sistema de fornecedor, com o qual interoperam, verificar estoques e registrar ordens de compra); b) *Interoperabilidade de Protocolo Total*, que permite a dois serviços substitutos passem a ser totalmente interoperáveis e se integrem, de modo que a troca de fornecedor para o paciente não traz qualquer diferença em termos de acesso aos serviços e entregas (por exemplo, diferentes clínicas médicas, ligadas a um mesmo grupo econômico, passam a ter seu sistema interoperável para ampliar de modo facilitado a gama de tratamentos disponíveis ao paciente); c) *Portabilidade de dados*, que a capacidade de um sujeito de dados de portar seus dados de um fornecedor de serviços para outro fornecedor de serviços; d) *Interoperabilidade de Dados*, que tem seu foco na possibilidade de acesso continuado e em tempo real aos dados de diferentes serviços, complementares ou substitutos.

---

7 Porter, Michael E., LEE, Thomas, H. The Strategy that will fix health care. Harvard Business Review, October 2013.

8 Palfrey, J., Gasser, U. Interop: The Promise and Perils of Highly Interconnected Systems, Basic Books, 1a ed. , 2012

Note que a interoperabilidade não significa, portanto, a centralização de dados, sendo, ao inverso, uma alternativa tecnológica à concentração, na medida em que permite que diferentes sistemas se comuniquem e sejam funcionalmente compatíveis. É claro que é possível tornar sistemas interoperáveis na medida em que acessem uma mesma base de dados centralizada, mas tal formato não é necessário e pode trazer mais riscos em relação a segurança. A interoperabilidade tampouco exige que diferentes organizações utilizem o mesmo sistema de tecnologia da informação.<sup>9</sup> Para que haja acesso contínuo e em tempo real aos dados relevantes, é suficiente que haja uma padronização de *metadados* e rotinas para que dados de um sistema sejam transmitidos ou visualizados e compreendidos corretamente pelo outro sistema.

Os países desenvolvidos e em desenvolvimento tem estimulado políticas sobre o sistema de saúde que enfatizam a adoção de prontuários eletrônicos interoperáveis, de modo a oferecer um atendimento mais direcionado, personalizado, efetivo e eficiente em custos, reduzindo erros, aumentando o sucesso de diagnósticos e tratamentos e evitando a duplicação de operações.<sup>10</sup> De acordo com a OCDE a capacidade de compartilhar dados entre provedores de cuidado e pacientes é um aspecto fundamental para elevar a segurança do paciente, reduzir o número de erros evitáveis e melhorar a coordenação e continuidade do cuidado<sup>11</sup>.

A interoperabilidade e acesso pelos profissionais de saúde autorizados ao histórico de saúde completo do paciente é benéfico para o sistema em dois lados: pelo lado do paciente, permite o conhecimento mais completo e acurado sobre seu estado e condições de saúde; pelo lado dos prestadores de serviços de saúde, permite maior eficiência e redução de custos ao evitar sobreposição de procedimentos.

O Brasil não é exceção, tendo o Ministério da Saúde destacado na Estratégia de Saúde Digital para o Brasil 2020-2028, dentre os seis pilares fundamentais para a saúde digital, a *informatização dos prontuários e a interoperabilidade* entre sistemas de atenção primária, laboratórios, farmácia, serviços de telemedicina e serviços ambulatoriais, por meio da estruturação da Rede Nacional de Dados de Saúde (RNDS), o desenvolvimento de padrões técnicos comuns e o fortalecimento do Repositório de Terminologias de Saúde (interoperabilidade semântica).

Nesse contexto de incentivo à digitalização de prontuários e a interoperabilidade de sistemas de atenção, reforça-se a coleta, tratamento e compartilhamento de dados pessoais de natureza sensível. Não só a informação presente nos prontuários é sensível como é também elevado o risco decorrente das inferências que podem ser obtidas sobre o perfil do sujeito do dado referido no prontuário, sobretudo com as metodologias de *data analytics* e inteligência artificial.<sup>12</sup>

---

9 Milieu L and Time.lex (2014) Overview of the national laws on electronic health records in the EU Member States and them

interaction with the provision of cross-border eHealth services Report. Brussels: 201/65.

10 Biancoletto, G. Data protection issues in cross border interoperability of electronic health record systems within the European Union. *Data & Policy*, v.2, 2020, doi:10.1017/dap.2020.2

11 OECD. New health Technologies-Managing Access, Value Sustainability (16 January 2017).

12 Com, efeito, pelo crescente emprego de inteligência artificial no setor, o processamento de dados

Não por outro motivo, a proteção de dados pessoais é uma das principais preocupações na implementação de um sistema de e-saúde (*e-health*) centrada no paciente e capaz de assegurar seus direitos fundamentais. Nos diferentes países em que há uma política de saúde digital, esta é acompanhada por uma série de salvaguardas para a proteção de dados pessoais, inclusive pela adoção de modelos de proteção de dados desde a concepção (*data protection by design* – DPbD) e proteção de dados por padrão (*data protection by default* – DPbDf) desde o estágio de desenvolvimento do prontuário eletrônico e do modelo de interoperabilidade.<sup>13</sup>

Essa preocupação tem motivado uma série de estudos e regulações em diversos países para assegurar o sigilo das informações, sua *cibersegurança* e o controle pelo *titular dos dados* sobre o fluxo de informações a seu respeito que podem ser extraídas dos dados presentes em prontuários eletrônicos (autodeterminação informacional).

No Brasil, há diferentes iniciativas no sentido de desenvolvimento de sistemas de *e-health*, baseadas no tratamento de dados de saúde a partir de prontuários eletrônicos, sendo necessário questionar, em que medida são compatíveis com a legislação nacional de proteção de dados, considerando, inclusive, a elevação da proteção de dados ao *status* de direito fundamental constitucional pela Emenda Constitucional 115/22.

Uma delas, que comporá o foco central deste estudo, está na requisição, por algumas Operadoras de Planos de Saúde (OPS), de compartilhamento do prontuário eletrônico, como condição para o cadastro de hospitais e clínicas que pretendam fazer parte da rede de estabelecimentos de saúde credenciados. Essa requisição é feita com base nos seguintes argumentos:

- a) O prontuário eletrônico compartilhado com a OPS permitiria a gestão de cuidado em medicina preventiva pela seguradora (veiculado em programas promocionais como “o médico da família”);
- b) Seria possível a interoperabilidade do prontuário eletrônico de modo que o beneficiário do plano de saúde poderia ter seu histórico acessado em diferentes unidades de atendimento cadastradas, aumentando a eficiência do tratamento;

passa não só a embasar a análise por profissionais de saúde, como também gerar sugestões de diagnóstico da presença atual de enfermidades ou mesmo fornecer a predição de enfermidade pelo quadro geral de saúde do paciente, além de ministrar automaticamente dosagens de medicamentos, sugerir terapias e assistir o médico na realização de intervenções cirúrgicas. Nos últimos anos, ocorreram desenvolvimentos significativos no uso de inteligência artificial para auxiliar os profissionais da saúde no diagnóstico médico e na tomada de decisões clínicas. O Brasil não é exceção, com o desenvolvimento de aplicativos que utilizam IA para classificar relatórios clínicos e fornecer diagnósticos automatizados, o que não está confinado a ambientes acadêmicos, possuindo aplicação tanto na saúde pública quanto na privada. Mas as inferências possíveis não se limitam aos usos médicos, podendo trazer informações chave para cálculos atuarias, por exemplo, pelas fontes pagadoras do sistema de saúde, bem como para uma série de inferências comportamentais Marco Almada and Juliano Maranhão. VOICE-BASED DIAGNOSIS OF COVID-19: ETHICAL AND LEGAL CHALLENGES. *International Data Privacy Law special issue on Data Protection in Latin America* (2021).

13 European Commission (2019) Commission Recommendation (EU) 2019/243 of February 6, 2019, on a European Electronic Health Record Exchange Format. Brussels: COM, 800 final

- c) O compartilhamento dos dados presentes no prontuário independeria de consentimento por parte do beneficiário do plano de saúde, pois encontraria sua base legal no art. 11, II, "f", da Lei Geral de Proteção de Dados Pessoais, uma vez que as OPSs poderiam ser enquadradas nos "serviços de saúde" mencionados naquele dispositivo.

Outra iniciativa consiste no Projeto de Lei 3814/2020, chamado projeto de lei do "prontuário único", que prevê a criação de plataforma digital única consolidando informações sobre histórico de saúde dos pacientes atendidos em estabelecimentos de saúde públicos ou privados. Uma terceira consiste na criação de sistema de OpenHealth que permitiria o compartilhamento de dados de saúde entre operadoras de planos de saúde, com o objetivo de ampliar a concorrência no mercado das OPSs.

Para o exame da compatibilidade da requisição de prontuários médicos por operadoras de saúde com o direito à proteção de dados pessoais, vale observar a experiência internacional em relação à implementação de projetos de *e-health* baseados na interoperabilidade de prontuários eletrônicos, bem como as restrições relativas ao compartilhamento de dados pessoais de saúde entre estabelecimentos de saúde e as fontes pagadoras, ou seja, seguradoras e fundos de saúde.

Dentre os sistemas estrangeiros escolhidos para o estudo estão: na Europa será primeiramente examinada a política geral da União Europeia em relação à saúde digital e o compartilhamento de dados à luz da General Data Protection Regulation (GDPR) e, em seguida, serão examinados os sistemas em alguns de seus principais países, como Alemanha, França, Espanha e Itália, tendo em vista que a GDPR abre espaço para a regulação específica pelos Estados-membros no que concerne a tratamentos baseados em cumprimento de lei; o Reino Unido, que também possui tradição em proteção de dados e uma regulação detalhada relativa a *e-health* e interoperabilidade; os Estados Unidos da América, que possuem um sistema de saúde, a exemplo do Brasil, com elevada participação de estabelecimentos de saúde e seguradoras privadas, além de contar com modelo avançado de *e-health*, acompanhado de forte regulação voltada para a proteção do sigilo e na autonomia dos pacientes; por fim, para um exemplo de país vizinho, já com tradição em proteção de dados pessoais, examinaremos a experiência argentina em relação à saúde digital, prontuários eletrônicos e interoperabilidade.

Após essa análise poderá ser acessado o mérito dos argumentos de promoção à interoperabilidade e gestão de cuidado. Em seguida procederemos à análise do sistema de saúde nacional e a exigência ou não de consentimento do titular do dado para o compartilhamento de prontuários médicos com operadoras de planos de saúde.

## 2. Experiência internacional em e-health, interoperabilidade de prontuários médicos e compartilhamento de dados com seguradoras

### 2.1. Europa

A Comissão Europeia tem dentre suas prioridades a estruturação e consolidação de sistema de *e-health* baseada em uma gestão eficiente de dados nos Estados-membros e no intercâmbio transfronteiriço, com a criação um Espaço Comum de Dados de Saúde, que, construído sobre bases transparentes, promova melhor intercâmbio e acesso a diferentes tipos de dados de saúde (registros eletrônicos de saúde, dados genômicos, dados de registros de pacientes, etc.), não apenas para apoiar a prestação de serviços de saúde, mas também para fins de pesquisa em saúde e elaboração de políticas de saúde. A infraestrutura a nível europeu seguirá a estratégia global do Espaço Europeu de Dados lançada pela publicação da estratégia europeia de dados em 19 de fevereiro de 2020<sup>14</sup>, ao mesmo tempo em que fornece uma análise aprofundada das especificidades do setor de saúde.

O Espaço Europeu de Dados de Saúde será construído, em cooperação entre a Comissão Europeia e os Estados-membros, sobre três pilares:

---

14 Cf.: [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy\\_pt](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_pt)

- i) Um forte sistema de governança e proteção de dados e regras para o intercâmbio de dados;
- ii) Garantia de qualidade dos dados;
- iii) Infraestrutura com padrões técnicos de interoperabilidade.

O pilar central de governança de dados está diretamente calcado no esforço de adequação ao Regulamento Geral de Proteção de Dados (GDPR) dos sistemas de dados, compartilhamento e interoperabilidade entre os atores envolvidos.

Os Estados-membros foram autorizados, por meio de cláusulas de especificação, a ajustar a aplicação de certos aspectos do regulamento à situação nacional. Além disso, o regulamento não exclui a legislação preexistente ou recém aprovada dos Estados-membros que estabelece circunstâncias para o processamento específico de categorias especiais de dados de interesse público. Os Estados-membros podem manter ou introduzir outras condições, incluindo limitações em relação ao processamento de, entre outros, dados relativos à saúde (Art. 9(4) GDPR).

Para fornecer uma estrutura para o uso dos dados de saúde nos Estados-membros, um trabalho preparatório foi conduzido em 2020, através de uma série de workshops e de um estudo<sup>15</sup>, e particularmente através de: (i) um mapeamento de como o GDPR é implementado no setor de saúde nos diferentes países, incluindo uma visão geral das modalidades legais e técnicas aplicáveis ao compartilhamento de dados de saúde para usos primários e secundários (ver definições abaixo) nos países da União Europeia (UE); (ii) uma visão geral das estruturas de governança existentes para o uso secundário de dados de saúde nos países da UE; (iii) recomendações para possíveis ações, legislativas e não legislativas, a nível da UE para facilitar o compartilhamento de dados de saúde em toda a UE para usos primários e secundários.

O objetivo da UE é melhorar a interoperabilidade e a padronização no intercâmbio de dados de saúde, mas os Estados-membros têm estruturas legais, abordagens e níveis de desenvolvimento da telemedicina que são muito heterogêneos, o que dificulta uma padronização eficaz das práticas a curto prazo. Além disso, os incidentes de uso indevido de dados por partes comerciais, incluindo aqueles ocorridos fora da UE, vêm aumentando a consciência de que o cumprimento das regras de proteção de dados deve ser assegurado. Daí a necessidade de uma consolidação de padrões técnicos e standards de linguagem para uma implementação de médio prazo.

O desafio para os Estados-membros e a UE como um todo é, portanto, encontrar um equilíbrio entre segurança, privacidade e compartilhamento de dados, considerando que este último é visto como um requisito fundamental para desenvolver inovações médicas.

O artigo 4(15) GDPR define dados relativos à saúde como dados pessoais relacionados à saúde física e mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre seu estado de saúde. Na prática, porém, os dados de saúde são frequentemente entendidos como quaisquer dados pessoais gerados den-

---

15 Cf.: [https://ec.europa.eu/health/system/files/2021-02/ms\\_rules\\_health-data\\_en\\_0.pdf](https://ec.europa.eu/health/system/files/2021-02/ms_rules_health-data_en_0.pdf)



tro dos sistemas de saúde, e alguns podem também incluir dados relativos à saúde que são coletados por cidadãos e pacientes por meio de dispositivos que possam ser vestíveis, aplicações e informações autorreportadas.

Em estudo sobre as bases legais utilizadas pelos Estados-membros para autorizar o tratamento de dados de saúde<sup>16</sup> faz-se referência a “uso primário” e “uso secundário” dos dados. Isso porque leis, regras e regulamentos diferentes podem ser aplicados dependendo do tipo e da finalidade do uso desses dados. O uso primário refere-se ao tratamento de dados específico para a finalidade de diagnóstico ou tratamento em procedimento médico realizado junto ao paciente, seja pelo próprio médico, seja pela clínica ou hospital. Já os usos secundários dizem respeito a reutilizações desses dados, seja para gestão do pagamento dos serviços, para fins de pesquisa ou para planejamento de políticas públicas de saúde. De acordo com o estudo, três funções amplas podem ser distinguidas envolvendo o processamento de dados de saúde, sendo o a função 1 considerada “uso primário” e as funções 2 e 3 consideradas “uso secundários”.

### 2.1.1 Usos primários

- Função 1: Processamento de dados para fins de prestação de assistência médica e social por prestadores de serviços de saúde e de assistência ao paciente.

Trata-se dos dados de saúde que são coletados diretamente de um paciente no contexto da prestação de serviços de saúde em um estabelecimento de saúde (clínica ou hospital) ou em uma mídia online (consulta remota). Esses dados incluem tanto aqueles de identificação, endereço e data de nascimento, como dados indicadores das condições de saúde e aspectos do tratamento, ou seja, incluindo dados sensíveis. Importante destacar que são dados especificamente coletados no ponto de cuidado e no contexto do procedimento médico. Esses dados coletados em um ponto de cuidado, podem ser necessários em outro ponto de cuidado por profissionais de saúde para a continuidade do tratamento, o que continua a se enquadrar nesta função, como uso primário.

Em relação ao uso primário, a base legal para tratamento empregada raramente se encontra no art. 6(1)(d) (interesse vital do titular dos dados), localizando-se mais no art. 6(1)(c) (cumprimento de obrigação legal, como no caso em que a legislação exige a coleta dos dados de saúde para registro em prontuários médicos hospitalares) ou em exceções à proibição geral de tratamento de dados sensíveis, como o art. 9(2)(h):

*“Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde...”*

Aqui fica especificada não só a finalidade de diagnóstico de saúde ou capacidade de trabalho por profissional de saúde, como a previsão deste tratamento em obrigação legal

---

16 Assessment of the EU Member States’ rules on health data in the light of the GDPR, European Commission, 2021.

ou em contrato de prestação de serviços médicos. Como se trata de obrigação legal ou contratual, não se indica o consentimento como base autorizadora do tratamento, tendo em vista que essa pressupõe o poder do titular do dado em retirar a autorização o objetar o uso sem qualquer detrimento a seus direitos.

O estudo destaca que o compartilhamento de dados de prontuários eletrônicos, dentro da função 1 e conforme a legislação dos países membros, não se dá por transferência, mas pela interoperabilidade no acesso. Ou seja, os prontuários eletrônicos são acessados por meio de plataforma por aqueles profissionais ou provedores de saúde autorizados. Estabelece-se tecnicamente uma espécie de hub, que não contém os dados, mas por meio do qual é possível acessar os prontuários de diferentes unidades de cuidado. Em alguns países, como na Holanda e Alemanha, existe ainda um controle granular do paciente sobre quais dados podem ser acessados por quais profissionais de saúde (o que tem criado algumas dificuldades para operação do sistema, por torná-lo por demasiado complexo).

Para viabilizar a interoperabilidade, segurança e qualidade dos dados, diferentes estados membro adotaram políticas, guias ou comandos legais estipulando padrões e standards para o sistema informático a ser empregado pelas organizações provedoras de cuidados médicos. Segundo o estudo, cerca de metade dos Estados-membros, que estão mais avançados em relação à interoperabilidade, foram adotados padrões técnicos para garantir que a estrutura e formato dos dados sejam interoperáveis e possam ser acessados por profissionais de saúde sem perda de conteúdo. Em alguns países esses standards são regionais e, em países mais atrasados no sistema de *e-health* não há a estipulação de padrões.

### **2.1.2 Usos secundários**

- Função 2: Processamento de dados para fins de saúde pública mais ampla, incluindo planejamento, gerenciamento, administração e melhoria dos sistemas de saúde e cuidados; prevenção ou controle de doenças transmissíveis; proteção contra ameaças graves à saúde e garantia de altos padrões de qualidade e segurança da saúde e de produtos e dispositivos médicos.
- Função 3: Processamento de dados para pesquisa científica ou histórica por organizações do setor público e privado. Processamento feito por terceiros, não sendo o controlador de dados original, incluindo as indústrias farmacêuticas e de tecnologia médica e os provedores de seguros.

As funções 2 e 3 dizem respeito à reutilização de dados de saúde que foram coletados inicialmente no contexto da prestação de cuidados, mas que podem posteriormente servir para outro propósito. Tal uso secundário pode ser exercido por entidades públicas, tais como pagadores legais dos sistemas nacionais de saúde (órgãos públicos de seguradoras de saúde), entidades públicas de pesquisa (incluindo universidades, laboratórios de saúde pública), por reguladores, tais como agências de medicamentos e organismos notificados, bem como pela indústria. O termo indústria inclui grandes e pequenas empresas farmacêuticas e de tecnologia médica, empresas do setor de seguros e serviços financeiros, como bem como os atores da mídia social e da eletrônica de consumo, e a emergente indústria de inteligência artificial. As funções 2 e 3 podem usar dados que permanecem nos repositórios de uso primário, como os sistemas de Registros Eletrônicos de Saúde, mas também podem ser reunidos em outros sistemas,

como os registros de doenças que coletam dados para calcular a incidência e prevalência da doença em nível nacional ou regional.

Nota-se que o termo “uso secundário” não é encontrado no GDPR, mas deve ser entendido como estando amplamente de acordo com o termo “processamento posterior” de dados, conforme descrito no princípio de limitação de finalidade estabelecido no artigo 5(1)(b). Isto estabelece que o processamento de dados para uma finalidade diferente daquela especificada no momento da coleta não será permitido quando for incompatível com a finalidade inicial, a menos que esse processamento adicional seja para (*inter alia*) fins de pesquisa e seja realizado de acordo com as salvaguardas descritas no Artigo 89(1) GDPR (minimização dos dados e adoção dos meios técnicos e organizacionais e podem incluir a pseudonimização para que não se permita a identificação dos titulares).

Naquele tipo de tratamento que mais interessa a este estudo, qual seja, a reutilização para gestão do sistema de saúde, incluindo planejamento de procedimentos e reembolso dos custos, o compartilhamento normalmente dependerá de legislação específica autorizando o uso ou decorrerá de tratamento necessário para o cumprimento de contrato, notadamente em caso de seguradoras privadas. Na ausência de legislação autorizadora ou de previsão contratual, o tratamento de dados por seguradoras de saúde deve se basear no *consentimento* do cliente<sup>17</sup>.

Todavia, o texto da Comissão Europeia destaca que esse uso secundário deve estar adequado aos critérios de *necessidade e proporcionalidade* (uso mínimo dos dados apenas naquilo necessário para atender a finalidade de planejamento e reembolso), além do dever de empregar medidas de *privacy by design e by default*<sup>18</sup> (art. 25 GDPR), que inclui, quando possível, a anonimização e pseudonimização. Obviamente que, em algumas formas frequentes de tratamento para essa finalidade, e.g. para reembolso ou análise de possível duplicação de tratamentos ou fraudes, a anonimização não é possível, mas a abrangência de dados deve, por meio de medidas técnicas e organizacionais, limitar-se ao estritamente necessário para a finalidade de reembolso.

---

17 É importante ter em mente que o consentimento é apenas uma das bases legais que autoriza o tratamento de dados pessoais, tanto no contexto do GDPR (Artigo 6º) quanto da LGPD (Art. 7º e 11). Embora seja possivelmente a base legal mais “conhecida”, nem sempre o consentimento será a base legal aplicável, principalmente nas hipóteses em que outra base legal puder justificar o tratamento dos dados. Além disso, não há (como estabelecido no senso comum) uma “hierarquia” de bases legais, o que significa dizer que nenhuma base legal é mais importante que outra, de modo que o tratamento não dependerá de uma base legal específica para ser levado a cabo, desde que haja alguma base legal aplicável.

18 *Privacy by design* e do *privacy by default* (em português, respectivamente, privacidade desde a concepção e privacidade por padrão) são dois princípios aplicáveis à proteção de dados pessoais, estabelecidos no Artigo 25 do GDPR, assim como no Art. 46, §2º e 49 da LGPD. Pelo princípio de *privacy by design*, todo o processo de desenvolvimento de um produto ou serviço que envolva o tratamento de dados pessoais deve garantir a proteção da privacidade. Segundo o princípio de *privacy by default*, o produto ou serviço que envolva o tratamento de dados deve ser comercializado com todas as salvaguardas de privacidade concebidas durante o seu desenvolvimento por padrão, isto é, deve ser fornecido observando as configurações de privacidade mais restritivas possíveis.

As futuras ações identificadas a nível da UE, que devem ser complementares e cumulativas, incluem códigos de conduta direcionados às partes interessadas, nova legislação direcionada e específica ao setor, orientação e apoio à cooperação entre os Estados-Membros e as partes interessadas relevantes, mas também apoio à digitalização, interoperabilidade e infraestruturas digitais, permitindo o acesso e o uso de dados para a saúde, elaboração de políticas e pesquisa e inovação. É importante que estas ações futuras sejam desenvolvidas no pleno respeito aos princípios de proporcionalidade e subsidiariedade

Há um bom nível de apoio para ações em nível da UE para promover o acesso e compartilhamento de dados de saúde. Tais medidas podem incluir uma combinação de leis brandas (através de um Código de Conduta) com outras ações não-legislativas e legislativas. Um Código de Conduta é considerado desejável para explicar conceitos do GDPR e para assegurar uma abordagem consistente ao intercâmbio de dados de saúde em um nível mais prático (por exemplo, definir formatos para o intercâmbio de dados).

## 2.2. França

### 2.2.1 Organização do sistema de saúde<sup>19</sup> francês

O sistema de saúde francês é centralizado, com responsabilidades regionais, baseado principalmente em um sistema de seguro social de saúde (SHI), com papel tradicionalmente forte para o Estado. Embora as agências regionais de saúde tenham desempenhado um papel maior na gestão da prestação de cuidados de saúde em nível local desde 2009, o SHI e o governo central sempre desempenharam um forte papel na organização do sistema de saúde e na determinação de suas condições operacionais. Nas últimas duas décadas, o Estado também se envolveu mais no controle dos gastos com saúde financiados pelo sistema SHI, estabelecendo uma meta nacional de gastos com saúde.

Em 2019, os sistemas públicos e privados de seguro de saúde obrigatório financiaram 83,7% de todos os gastos com saúde na França (mais do que a média da UE de 79,7%). A receita destes esquemas vem principalmente das contribuições à seguridade social pagas por empregadores e empregados, impostos de renda e fontes adicionais como os impostos sobre tabaco e álcool. Desde 1996, o crescimento anual dos gastos com SHI tem sido controlado pela meta nacional de gastos com saúde. Permaneceu constante em torno de 2,5% de crescimento por ano em 2009-19, mas cresceu 9,5% em 2020 devido a gastos adicionais relacionados à pandemia e à introdução de um novo plano de investimento para fortalecer os hospitais públicos.

O seguro social de saúde francês cobre toda a população. O sistema SHI oferece cobertura a toda a população com base na residência através de vários esquemas obrigatórios. O fundo principal (Caisse Nationale d'Assurance Maladie, CNAM) cobre 92% da população; o fundo agrícola cobre outros 7%. Outros fundos pequenos (específicos para

---

19 Cf.:

<https://www.oecd-ilibrary.org/docserver/7d668926-en.pdf?expires=1644660909&id=id&accname=guest&-checksum=9FB3FA5D32D9A613ECAA5CEA3AAAA377>

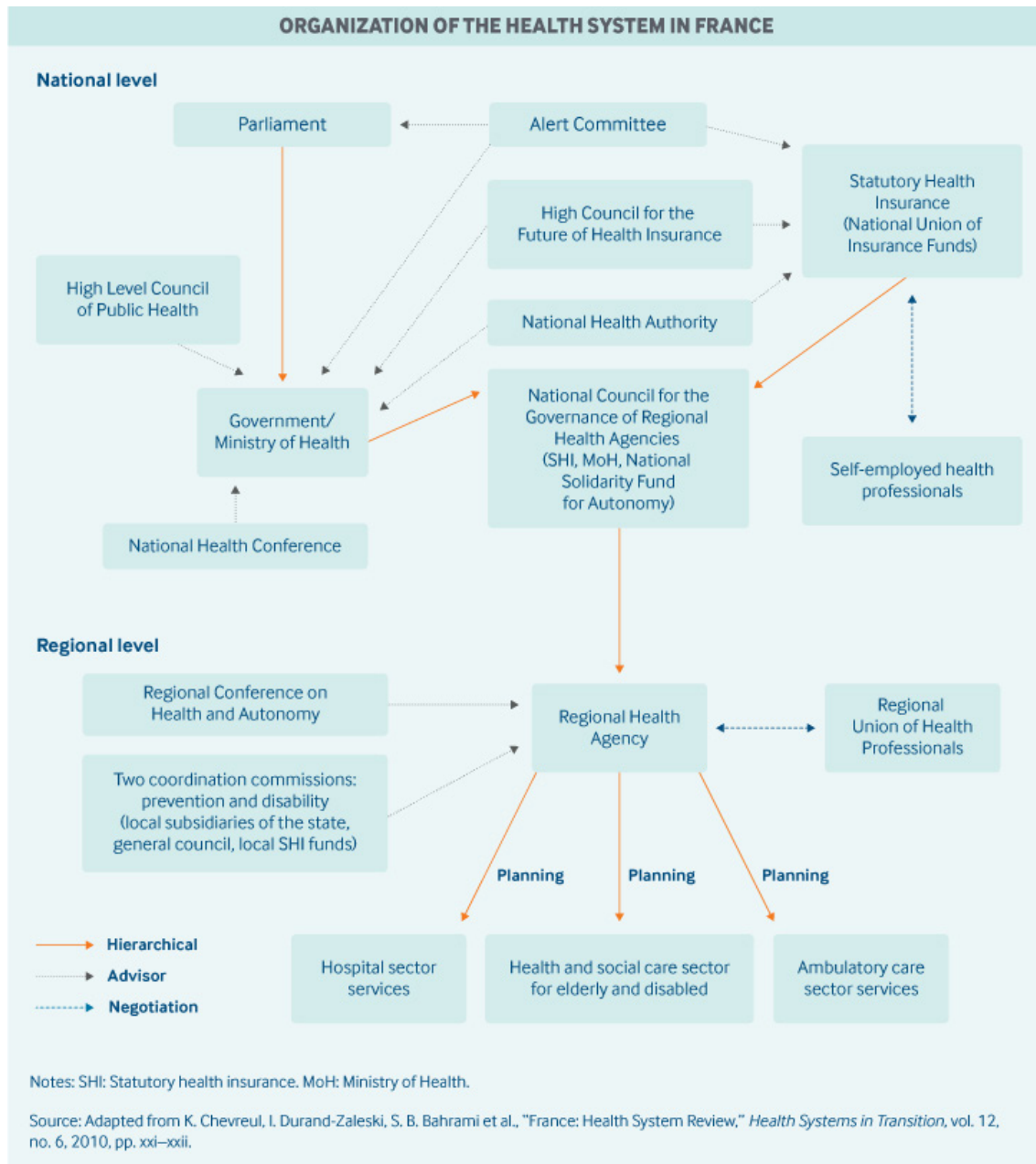
certas categorias profissionais, como a empresa ferroviária nacional) cobrem os 1 % restantes. Há também um esquema totalmente financiado pelo Estado que dá acesso a um pacote de benefícios específicos (cuidados essenciais) para migrantes indocumentados. Quase toda a população (95%) tem seguro de saúde complementar, principalmente para cobrir copagamentos e para obter melhor cobertura para bens e serviços médicos mal cobertos pelo SHI, tais como cuidados odontológicos e óticos.

A França vem progredindo em direção a uma cobertura de saúde universal: em 2015, o parlamento francês aprovou uma lei que visava a aumentar a universalidade da cobertura sanitária e a uniformidade da proteção em todas as caixas de previdência. Uma das principais conquistas desta reforma foi garantir a continuidade da cobertura de saúde quando as pessoas enfrentam uma mudança em sua situação profissional ou pessoal.

A França reporta a menor proporção de despesas extras para o cidadão para saúde entre todos os países da UE (9,3% em comparação com a média de 15,4% da UE) porque os planos de seguro de saúde públicos e privados cobrem a maior parte dos gastos com saúde.

Cada estabelecimento de saúde pública é parte de um acordo de agrupamento hospitalar territorial (GHT) por uma gestão comum local. O estabelecimento suporte do GHT é responsável pela gestão conjunta do sistema convergente de informações hospitalares entre as instituições envolvidas. Em particular, ele administra a implementação de um arquivo informatizado do paciente, permitindo o gerenciamento coordenado do paciente dentro das instituições pertencentes ao GHT.

Abaixo, um infográfico<sup>20</sup> ilustrando a organização do sistema de saúde francês:



## 2.2.2 O sistema francês de dados de saúde

Na França, a proteção de dados pessoais é regida pela lei de 6 de janeiro de 1978 conhecida como "Informatique et Libertés".<sup>21</sup> A lei de 20 de junho de 2018<sup>22</sup> sobre a proteção de dados pessoais alterou a lei "Informatique et Libertés" para adaptá-la às disposições da GDPR.

O sistema nacional de dados de saúde francês (SNDS) foi criado em 2016 para desenvolver o uso de dados de saúde e constitui um avanço considerável na análise e melho-

20 Cf.: <https://www.commonwealthfund.org/international-health-policy-center/countries/france>

21 Cf.: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/>

22 Cf.: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952>

ria da saúde da população. Administrado pela Caisse Nationale de l'Assurance Maladie (CNAM), o SNDS melhora o sistema de informações históricas da CNAM e permite que novos dados sejam referenciados:

- i) Dados do seguro saúde (banco de dados do sistema nacional de informações sobre seguro saúde Interregime - SNIIRAM);
- ii) Dados hospitalares (banco de dados do programa de medicalização dos sistemas de informação - PMSI) historicamente coincidiram com o Sniiram;
- iii) Bancos de dados sobre as causas médicas de morte (banco de dados do centro de epidemiologia sobre as causas médicas de morte do instituto nacional de saúde e pesquisa médica - CépiDc do Inserm);
- iv) Dados relativos à deficiência (das *Maisons Départementales des Personnes Handicapées* – MDPH; dados da *Caisse Nationale de Solidarité Pour L'autonomie* - CNSA).

O SNDS enriquece o sistema nacional de informação interregimes de seguros de saúde (Sniiram), acrescentando novos dados, ampliando o histórico, facilitando os processos de acesso aos dados e autorizando novos propósitos. O objetivo do SNDS é disponibilizar esses dados para promover estudos, pesquisas ou avaliações de interesse público e contribuir para um dos seguintes propósitos: (i) informações sobre saúde; (ii) a implementação de políticas de saúde; (iii) conhecimento dos gastos com saúde; (iv) informações para profissionais e instituições sobre suas atividades; (v) inovação nos campos da saúde e do atendimento médico-social; (vi) vigilância, monitoramento e segurança sanitária.

São especificamente proibidos os seguintes tratamentos:

- i) Todos os propósitos que resultariam em uma decisão tomada contra uma pessoa identificada com base nos dados que lhe dizem respeito e que apareçam em uma dessas operações de processamento, ou que visariam: a) a promoção de produtos de saúde para profissionais ou instituições de saúde; ou b) a exclusão de garantias de contratos de seguro ou a modificação de contribuições ou prêmios de seguro para um indivíduo ou um grupo de indivíduos.

### 2.2.3 “Mon Espace Santé”

Em 3 de fevereiro de 2022, o governo lançou oficialmente um novo serviço público, chamado “Mon Espace Santé”, que visa a substituir e melhorar o arquivo médico pessoal compartilhado (*Dossier Medical Partagé* - DMP) lançado em 2004, mas que não obteve adesão. “Mon Espace Santé” é um serviço digital individual e personalizável para todos os usuários do sistema de saúde. Permite que todos armazenem e compartilhem seus documentos e dados de saúde com grau máximo de segurança. Os dados são hospedados na França, sob a proteção do Estado e do Seguro Saúde.

Atualmente o serviço inclui:

- i) um arquivo médico, para armazenar dados de saúde com segurança: perfil médico, medidas de saúde, tratamentos, resultados de testes, registros de va-

cinação, histórico médico, relatórios de hospitalização etc. e compartilhá-los com os profissionais de saúde, especialmente em caso de emergência;

- i) um sistema seguro de mensagens para troca de informações com profissionais de saúde em total confidencialidade.

Além do segurado, somente profissionais de saúde terão acesso ao DMP, o que exclui formal e explicitamente, por exemplo, as seguradoras de saúde e os empregadores.

Para acessar o espaço de um paciente, os cuidadores devem se identificar com um cartão magnético e devem primeiro solicitar uma autorização oral ou escrita. Em seguida, os membros de sua equipe médica serão automaticamente autorizados a consultar o espaço do paciente: as pessoas envolvidas no atendimento do paciente no mesmo hospital ou centro de atendimento, assim como os profissionais recomendados por seu médico, sejam eles enfermeiros, fisioterapeutas ou outras profissões médicas autorizadas.

Observe que, em uma emergência, se o segurado estiver confuso ou inconsciente, qualquer profissional de saúde está autorizado a acessar seu espaço, a menos que ele tenha se oposto a este princípio na seção *Acesso de emergência*.

#### **2.2.4 Interoperabilidade no sistema de saúde francês**

Como parte da estratégia “*Ma santé 2022*” para transformar o sistema de saúde (STSS) e seu componente digital, o Ministère de la Santé et des Solidarités publicou o documento “*Doctrine du Numérique en Santé, Version 2021*”<sup>23</sup>, cujo objetivo é descrever a estrutura técnica em que serviços digitais para o intercâmbio e compartilhamento de dados de saúde devem ser inscritos.

Para que a comunicação desmaterializada seja possível, todos os atores e, sobretudo, todos os seus sistemas de informação devem se valer de linguagem e terminologias padrão para serem interoperáveis. A estrutura de interoperabilidade é uma condição necessária para que os sistemas de informação hospitalar sejam capazes de distinguir entre relatórios e prescrições ou boletins de alta sem capacidade de leitura e é um pré-requisito para um atendimento consistente e eficiente ao paciente.

A interoperabilidade objetivada consiste na *interoperabilidade de dados*, abrangendo as esferas técnica e semântica, com controle de acesso atribuído ao próprio paciente e limitado a profissionais de saúde. É sobre essas bases semânticas e sintáticas que os fabricantes desenvolvem serviços de valor agregado retrabalhando os dados (curvas de tendência temporal, suporte à decisão, processamento automático da linguagem natural, inteligência artificial, por exemplo).

De acordo com o documento (capítulo “3. *Interopérabilité des systèmes d’information de santé*”), o Estado define os parâmetros para a interoperabilidade “técnica” e “semântica” dos sistemas de informação sanitária:

---

23 Cf.: [https://esante.gouv.fr/sites/default/files/media\\_entity/documents/doctrine-du-numerique-en-sante\\_version-2021\\_fevrier-22\\_vf.pdf](https://esante.gouv.fr/sites/default/files/media_entity/documents/doctrine-du-numerique-en-sante_version-2021_fevrier-22_vf.pdf).



- i) O Estado indica os principais princípios gerais da interoperabilidade: O conjunto de especificações de interoperabilidade e terminologias constitui um bem comum, que deve respeitar o princípio de transparência, colaboração, participação e ética. Os princípios gerais da doutrina da interoperabilidade são:
  - a) Princípio da transparência: produtos em OpenData, licença aberta ETALAB; equidade de tratamento entre industriais
  - b) Princípio da colaboração: concertação de produtos; transversalidade das *expertises*
  - c) Princípios de participação: co-construção de produtos com o ecossistema; avaliação de ações e produtos
  - d) Princípios éticos: respeito ao marco legal; respeito aos direitos dos pacientes e dos usuários; equidade de tratamento entre os atores.
- i) O Estado confia à Agence du Numérique en Santé (ANS) a tarefa de organizar a representação da França nos organismos internacionais de interoperabilidade e normalização.
- ii) Para intensificar o compartilhamento e o intercâmbio de dados de saúde entre soluções, o Estado confia à ANS a responsabilidade de desenvolver e publicar repositórios de interoperabilidade.
- iii) O Estado está seguindo uma política proativa para fazer cumprir os repositórios de interoperabilidade.
- iv) O Estado está seguindo uma política proativa para impor normas de interoperabilidade.

### **2.2.5 Seguro saúde e dados pessoais na França**

Quando os segurados fazem um contrato de seguro saúde suplementar, as companhias de seguros coletam dados pessoais, mediante consentimento do contratante que podem provir de duas fontes principais e podem ser usados para finalidades e formas de tratamento previstas em lei:

- i) Os formulários a serem preenchidos como parte do contrato complementar de saúde. As organizações pedem aos assinantes que forneçam informações sobre seu perfil pessoal (idade, sexo, local de residência, profissão), mas também sobre seu perfil médico através de um questionário de saúde, a fim de avaliar melhor o risco (histórico de doenças graves, doenças crônicas, práticas profissionais ou esportivas de risco, consumo de álcool ou tabaco etc.). Tais dados dizem respeito a muitos indivíduos, dada a obrigação dos empregadores privados de fazer um seguro mútuo para seus empregados.
- ii) Objetos conectados. Eles fazem parte da vida cotidiana na França: relógios inteligentes, pulseiras inteligentes, balanças conectadas – todos ligados a aplicações móveis que monitoram a atividade física em tempo real e enviam toneladas de dados sobre a saúde do usuário. Eles permitem que as companhias

de seguros e as companhias de seguros complementares de saúde tenham uma ideia do estilo de vida de seus segurados – com o consentimento destes últimos - a fim de adaptar seus preços e/ou condições contratuais.

Estes dados são de natureza sensível. Por esta razão, seu uso é estritamente regulamentado: o dado só pode ser usado para um propósito específico, anunciado aos indivíduos com antecedência e por um período limitado, conforme estabelecido por lei. Devem ser comunicados somente às pessoas e organizações envolvidas (subcontratados ou parceiros, pessoal autorizado da mútua, delegados, prestadores de serviços, resseguradoras, organizações sociais etc.). E sua segurança deve ser garantida em todos os níveis.

Para as organizações de seguro saúde complementar<sup>24</sup>, o acesso e o compartilhamento de dados de saúde é um grande desafio, respeitando as liberdades individuais, as regras éticas e deontológicas relativas ao seu uso e as regulamentações em vigor, na medida em que devem permitir (i) participação no gerenciamento de riscos à saúde através do conhecimento dos dados de saúde de reembolso; (ii) contribuir para a reflexão e ação sobre o desenvolvimento do sistema de saúde, sua organização e funcionamento (assistência ao paciente, caminhos de cuidados, métodos de pagamento, etc.); e (iii) a boa governança do sistema de saúde, que requer conhecimento compartilhado de como ele funciona e como é financiado. De acordo com a União dos seguros complementares de saúde da França, o acesso aos dados de saúde para as organizações de saúde complementares permanece limitado, o que torna esses importantes atores do sistema de saúde “pagadores cegos”, mesmo considerando que a lei no. 2019-774 de 24 de julho de 2019<sup>25</sup> sobre a organização e transformação do sistema de saúde, tenha confirmado o princípio da abertura dos dados de saúde.

No entanto, para a autoridade francesa de proteção de dados, a CNIL - Commission Nationale de L’informatique et des Libertés, somente os dados relevantes e necessários para a finalidade do contrato no contexto de um contrato de seguro devem ser processados. Quando se trata do processamento de dados ligados ao número de seguridade social e de saúde, deve-se ter um cuidado especial.<sup>26</sup>

De acordo com a CNIL, em sua página dedicada a dados acessíveis por organizações no setor de seguros<sup>27</sup>, os responsáveis pelo tratamento de dados devem processar dados de identificação, dados relativos à gestão do contrato, situação familiar, situação econômica, patrimonial e financeira, etc. somente quando forem relevantes e estritamente necessários em relação à finalidade do processamento no contexto dos dois conjuntos de finalidades: (1) conclusão, gestão e execução de contratos de seguro; e (2) a prospecção comercial por organizações de seguros.

Por exemplo, para o primeiro conjunto de finalidades, no contexto da conclusão, gestão ou execução de um contrato de seguro saúde suplementar, não são necessá-

---

24 Cf.: <https://unocam.fr/nos-actions/plateforme-donnees-sante/>

25 Cf.: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000038821260/>

26 Cf.: <https://www.cnil.fr/fr/le-principe-de-minimisation-et-les-traitements-du-nir-et-des-donnees-de-sante-dans-le-secteur-de>

27 Cf.: <https://www.cnil.fr/fr/le-principe-de-minimisation-et-les-traitements-du-nir-et-des-donnees-de-sante-dans-le-secteur-de>

rios dados relativos à localização do bem segurado. Os dados sensíveis não são considerados necessários.

Além da aplicação do princípio da minimização, o processamento de certas categorias de dados está sujeito a restrições específicas, como o número de seguridade social, cujo uso fora dos casos de uso referidos por decreto (por exemplo, no setor de saúde ou social) é proibido. Este também é o caso de dados sensíveis, como dados de saúde, cujo processamento é, em princípio, proibido, apesar de certas derrogações quando expressamente previstas em lei e para a finalidade específica de atuação da instituição.

## 2.3 Espanha

### 2.3.1 Organização do sistema de saúde<sup>28</sup> espanhol

A Espanha tem um sistema de saúde descentralizado com coordenação nacional. O sistema nacional de saúde - Sistema Nacional de Saúde (SNS) - é baseado na cobertura universal e é financiado principalmente por impostos. O sistema público oferece cuidados básicos de saúde gratuitos àqueles que contribuem para o sistema de seguridade social espanhol e suas famílias. O sistema público também oferece assistência médica gratuita para aposentados, incluindo os de outros países da UE.

Enquanto o planejamento e a regulamentação nacional continuam sendo de responsabilidade do Ministério da Saúde, as competências sanitárias e a jurisdição primária sobre o planejamento operacional em nível regional, a alocação de recursos, compras e provisão são devolvidas às 17 autoridades sanitárias regionais (das comunidades autônomas). Tais autoridades regionais muitas vezes contam com o apoio de agências nacionais especializadas, como a Rede de Agências para a Avaliação de Tecnologias e Benefícios da Saúde. O Conselho Interterritorial SNS, que compreende o ministro nacional e os 17 ministros regionais da saúde, é responsável pela coordenação de alto nível das ações em todos os sistemas regionais de saúde.

Os gastos da Espanha com saúde aumentaram nos últimos anos, mas permanecem abaixo da média da UE. O financiamento público como proporção dos gastos totais com saúde foi de 70,6% em 2019, o que é uma proporção menor do que a média da UE de 79,7%. Embora a proporção dos gastos públicos com saúde tenha diminuído de 75,1% em 2009 para 70,3% em 2014, como resultado das medidas de redução de custos e maior copagamento de medicamentos introduzidas após a crise econômica de 2009, ela começou a aumentar novamente nos últimos anos. Após uma revisão em 2012, as taxas de divisão de custos para os pacientes foram aumentadas e calculadas de acordo com o nível de renda e status de emprego, incluindo limites mensais para proteger os pensionistas. Importantes isenções para outros grupos vulneráveis também foram introduzidas e ampliadas nos últimos anos.

---

28 Cf.: <https://www.oecd-ilibrary.org/docserver/7ed63dd4-en.pdf?expires=1644661449&id=id&accname=guest&checksum=466C4FF38E2DB623C7D8A160DB555E03>

Na Espanha, as regiões têm total responsabilidade pelo planejamento e desenvolvimento de serviços de saúde digitais. Antes da pandemia, a maioria dos sistemas regionais de saúde já tinha implementado receitas eletrônicas, prontuários eletrônicos de saúde e portais *web* ou aplicativos móveis através dos quais os cidadãos podem acessar seus dados de saúde e gerenciar suas consultas médicas.

### 2.3.2 O sistema nacional de dados de saúde espanhol

Além do GDPR, a principal lei nacional de proteção de dados da Espanha é a Lei Orgânica 3/2018, de 5 de dezembro, sobre a Proteção de Dados Pessoais e o Proteção de dados pessoais e garantia dos direitos digitais.<sup>29</sup>

O SNS embarcou em ambicioso programa de modernização tecnológica, para o qual foi estabelecida uma nova Secretaria Geral de Saúde Digital, Informação e Inovação. Seus principais objetivos são o desenvolvimento de serviços públicos digitais, melhoria da saúde eletrônica (*e-health*), melhoria da interoperabilidade dos sistemas de informação clínica e de saúde com bancos de dados nacionais e internacionais, promoção da inovação e reforço das capacidades de avaliação de desempenho e análise de dados. Esta iniciativa é consistente com o plano de desenvolver um Espaço Europeu de Dados de Saúde para promover melhor intercâmbio e acesso a diferentes tipos de dados de saúde (tais como registros de saúde eletrônicos, dados genômicos, dados de registros de pacientes etc.), e para apoiar a prestação de serviços de saúde, pesquisa em saúde e elaboração de políticas.

A Lei 41/2002 de 14 de novembro de 2002<sup>30</sup> é a lei básica que regula a autonomia do paciente e os direitos e obrigações referentes à informação e documentação clínica (Lei de Autonomia do Paciente - LAP) como: o conjunto de documentos contendo dados, avaliações e informações de qualquer tipo sobre a situação e a evolução clínica de um paciente durante todo o processo de atendimento.

Após o processo de atendimento, o paciente e as informações clínicas correspondentes são devolvidas ao médico de atendimento primário que, por ter todos os dados da biografia de saúde do paciente, garante a visão geral clínica e terapêutica. Isto permite que a continuidade do atendimento seja caracterizada pela equidade, independentemente do local de residência e das circunstâncias individuais de autonomia, já que o atendimento pode ser prestado na própria casa do paciente.

Todas essas informações pessoais e de saúde constituem a chamada "história clínica", que é definida pela LAP. A história clínica compreende o conjunto de documentos relativos aos processos de atendimento de cada paciente, com a identificação dos médicos e outros profissionais que neles intervieram, com o objetivo de obter a máxima integração possível da documentação clínica de cada paciente, pelo menos no nível de cada centro de saúde. O registro clínico deve incorporar as informações consideradas importantes para o conhecimento exato e atualizado do estado de saúde do paciente. Todos os pacientes ou

29 Cf.: <https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf>

30 Cf.: <https://www.boe.es/buscar/act.php?id=BOE-A-2002-22188>

usuários têm o direito de ter um registro escrito, ou no suporte técnico mais apropriado, das informações obtidas em todos os seus processos de saúde, realizado pelo serviço de saúde tanto no atendimento primário como no atendimento especializado. O principal objetivo do prontuário médico é facilitar o atendimento médico, registrando todos os dados que, de acordo com critérios médicos, permitem um conhecimento preciso e atualizado do estado de saúde referido no parágrafo anterior.

As pessoas/pacientes têm o direito de contatar o controlador do processamento de seus dados (médicos, centros de saúde, tanto públicos como privados) solicitando acesso à documentação que constitui seus registros médicos.

A LAP estabelece algumas particularidades em relação ao acesso aos prontuários médicos. O direito de acesso do paciente à documentação da história clínica não pode ser exercido em detrimento do direito de terceiros à confidencialidade dos dados nela coletados no interesse terapêutico do paciente, nem em detrimento do direito dos profissionais envolvidos em sua preparação, que podem se opor ao direito de acesso a confidencialidade de suas notas subjetivas.

O controlador (geralmente o médico, instituição de saúde ou administração de saúde) e o processador (prestadores de serviços externos, como aqueles que realizam exames de sangue e outros exames que foram contratados a terceiros, por exemplo) devem tomar as medidas necessárias para garantir que qualquer pessoa agindo sob sua autoridade e tendo acesso aos dados pessoais só pode processar tais dados somente de acordo com suas instruções. Quando um profissional de saúde acessa um registro médico deve fazer isso porque é necessário para realizar seu trabalho.

### **2.3.3 Interoperabilidade no sistema de saúde espanhol**

A Secretaría General de Salud Digital, Información e Innovación para el SNS, do Ministerio de Sanidad da Espanha publicou, em dezembro de 2021, o documento “Estrategia de Salud Digital”.

A Estratégia constitui o quadro de referência para o desenvolvimento das diferentes iniciativas e ações das administrações de saúde competentes, promovendo o Sistema Nacional de Saúde para abordar sua transformação digital de forma harmoniosa e coordenada. A Estratégia se concentra principalmente em quatro objetivos estratégicos:

- i) Capacitar e envolver pessoas em seus cuidados de saúde e controle de doenças e facilitando sua relação com os serviços de saúde, promovendo sua participação em todos os níveis e fomentando sua corresponsabilidade.
- ii) Maximizar o valor dos processos para melhorar o desempenho e a eficiência do sistema de saúde pública, apoiando o trabalho dos profissionais e facilitando a comunicação entre eles a fim de garantir a continuidade dos cuidados e fortalecer a governança das organizações.
- iii) Adotar políticas de gerenciamento de dados e governança que permitam a disponibilidade de informações interoperáveis e de qualidade e criar um Espaço Nacional de Dados de Saúde para a geração de conhecimento científico e a avaliação dos serviços.

- iv) Adaptar a evolução do SNS às exigências da sociedade atual, aplicando políticas de inovação voltadas para a medicina 5P (População, Preventiva, Preditiva, Personalizada e Participativa).

Sobre a interoperabilidade, o documento indica que a transformação digital deve garantir que todos os dados gerados no e pelo NHS estejam disponíveis para serem transformados em informações interoperáveis e de qualidade entre os atores dedicados ao seu uso primário, consistente na prestação de serviços de saúde e assistência à saúde. O princípio de dados FAIR (*findable, accessible, interoperable and reusable*) derivados do campo de pesquisa, juntamente com a proteção adequada dos dados pessoais e o desenvolvimento e aplicação de padrões éticos em seu processamento, devem sustentar o desenvolvimento do digital serviços de saúde digitais.

Por um lado, o objetivo é fortalecer os sistemas de vigilância da saúde pública, de modo a gerar maior capacidade de coordenação, imediatismo e previsibilidade a fim de antecipar os riscos e apoiar a antecipação de riscos e apoio à decisão das autoridades sanitárias.

Por outro lado, aos envolvidos – profissionais e pacientes – deve ser assegurada a disponibilidade das informações necessárias para um trabalho melhor e mais seguro na promoção da saúde, prevenção de doenças e deficiências e cuidados com a saúde, incluindo também aspectos de ensino e pesquisa.

Da mesma forma, promover a saúde para melhores resultados, através da análise avançada de dados que devem proporcionar retornos de conhecimento aos profissionais e promover o trabalho dos pesquisadores para o desenvolvimento científico no campo da saúde, em particular para aumentar a robustez das provas científicas para a tomada de decisões em saúde pública.

Para tornar possível a construção do Espaço de Dados, a definição e padronização dos conceitos de vigilância, prevenção, cuidado e gerenciamento devem ser ampliados e a “onicanalização” assegurada, ou seja, que os dados de saúde das pessoas sejam comuns e transversais, independentemente do ponto de coleta ou acesso e de acordo com as disposições do atual marco regulatório para a proteção de dados pessoais.

### **2.3.4 Seguro Saúde e dados pessoais na Espanha**

Os dados de saúde podem ser divulgados a outras entidades além daquelas envolvidas no ponto de coleta, que são os hospitais e clínicas médicas, se houver uma base legítima para fazê-lo.

De acordo com o Guia para Pacientes e Usuários da Saúde<sup>31</sup>, não é necessário que o médico ou instituição de saúde solicite o consentimento dos pacientes para a coleta e uso de dados pessoais e de saúde se estes forem utilizados para fins de medicina preventiva ou ocupacional, avaliação da capacidade de trabalho do trabalhador, diagnóstico médico, prestação de assistência ou tratamento médico ou social, ou gestão de sistemas e serviços

31 Cf.: <https://www.aepd.es/sites/default/files/2019-12/guia-pacientes-usuarios-sanidad.pdf>

de saúde e assistência social. Nesses casos, como não há o consentimento do paciente, o tratamento deverá ser justificado mediante outra base legal: a do artigo 6(1)(b) do GDPR (execução de um contrato), nos casos de tratamento de dados por instituições privadas; ou a do artigo 6(1)(c) da mesma norma (cumprimento de obrigação legal), se o tratamento for realizado no âmbito da saúde pública.

Também não é necessário se o processamento de dados for realizado por razões de interesse público no campo da saúde pública, tais como a proteção contra ameaças graves à saúde transfronteiriças, ou para garantir altos padrões de qualidade e segurança da saúde e de produtos medicinais ou dispositivos médicos, ou a inspeção de reclamações dos cidadãos. Nessa hipótese, a base legal para o tratamento será aquela estabelecida no artigo 6(1)(e) do GDPR, que estabelece que o tratamento é lícito quando “for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento”.

Já com relação a gestão do pagamento, embora o consentimento não seja necessário, o conjunto de dados a serem transferidos é limitado pelos princípios de necessidade e proporcionalidade. Por exemplo, no caso de uma consulta médica remunerada por uma seguradora privada, o médico que cuida do paciente fornecerá os dados mínimos necessários para que a seguradora pague ao paciente pelo serviço prestado. Além disso, em que pese o compartilhamento de dados poder ser fundamentado em diferentes bases legais, é necessário garantir e informar ao paciente sobre uma série de direitos que este possui, como: a identidade e as informações sobre o responsável pelo tratamento; os dados de contato do encarregado de proteção de dados (“DPO”), nas hipóteses em que este for exigido; informações sobre as finalidades do tratamento; os destinatários ou as categorias de destinatários aos quais os dados são confiados; a intenção do responsável pelo tratamento de transferir os dados para outro país ou organização internacional; a duração do tratamento dos dados; o direito de acesso aos dados; o direito de retirar o consentimento, nas hipóteses em que o tratamento for justificado por meio dessa base legal; o direito de objeção e reclamação perante à autoridade de controle; e informações sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

## 2.4 Alemanha

### 2.4.1 Organização do sistema de saúde alemão

O sistema de saúde alemão é um sistema dual público-privado, instaurado no final do Século XIX, o que o torna o mais antigo da Europa<sup>32</sup>. O sistema de saúde na Alemanha é financiado por contribuições estatutárias, podendo ser complementado mediante a contratação de planos de saúde privados (*private Krankenversicherung* ou PKV) para substituir ou complementar a cobertura estatal (*gesetzliche Krankenkasse* ou GKV). O Ministério Federal da Saúde é responsável pelo desenvolvimento da política de saúde na Alemanha, e o setor é regulamentado pelo Comitê Federal Conjunto, embora o Governo não tenha praticamente nenhum papel na prestação direta de serviços de saúde.<sup>33</sup>

Todos os residentes alemães têm acesso ao sistema de saúde através do seguro de saúde público. Aproximadamente 86% da população está inscrita no seguro de saúde obrigatório, que fornece cobertura de internação, ambulatorio, saúde mental e medicamentos prescritos. A administração é feita por seguradoras não-governamentais conhecidas como *Krankenkasse/Krankenversicherung* (termo que poderia ser traduzido livremente como "fundo de seguro de saúde", ou "unidade de seguro de saúde").

A adesão ao seguro de saúde público obrigatório (GKV) e ao seguro de saúde privado (PKV) tornaram-se obrigatórios em abril de 2007. A partir de janeiro de 2009, todas as pessoas residentes na Alemanha foram obrigadas a fazer um seguro de saúde. Trabalhadores são obrigados a fazer contribuições ao GKV se sua renda estiver abaixo de um certo nível (em 2020 o limite era de 5.212,50 euros por mês). Se sua renda mensal exceder este nível, os funcionários podem manter o GKV voluntariamente ou optar por fazer um seguro de saúde privado (atualmente, os alemães que ganham mais de 68.000 euros anualmente podem optar por não se inscrever no sistema público e escolher um seguro de saúde privado, para os quais não há subsídios governamentais).

O seguro de saúde obrigatório faz parte do sistema de previdência social alemão. Seus fundos são diretamente responsáveis por prestar o serviço de seguro a seus membros, além de promover iniciativas de saúde preventiva e de melhoria de qualidade de vida. As seguradoras de saúde privadas, por sua vez, são empresas do setor privado que oferecem seguros de saúde, com contratos que complementam ou substituem o seguro de saúde obrigatório. Tanto o GKV como o PKV são financiados por contribuições de seus membros, com a diferença que, enquanto o valor da contribuição para o PKV depende de fatores como saúde de uma pessoa, a idade em que ela faz o seguro, seu risco individual, o tipo de cobertura e qualquer excesso, as contribuições para GKV são baseadas no salário de uma pessoa. Além disso, com o GKV, todos os segurados recebem o mesmo nível de serviços.

---

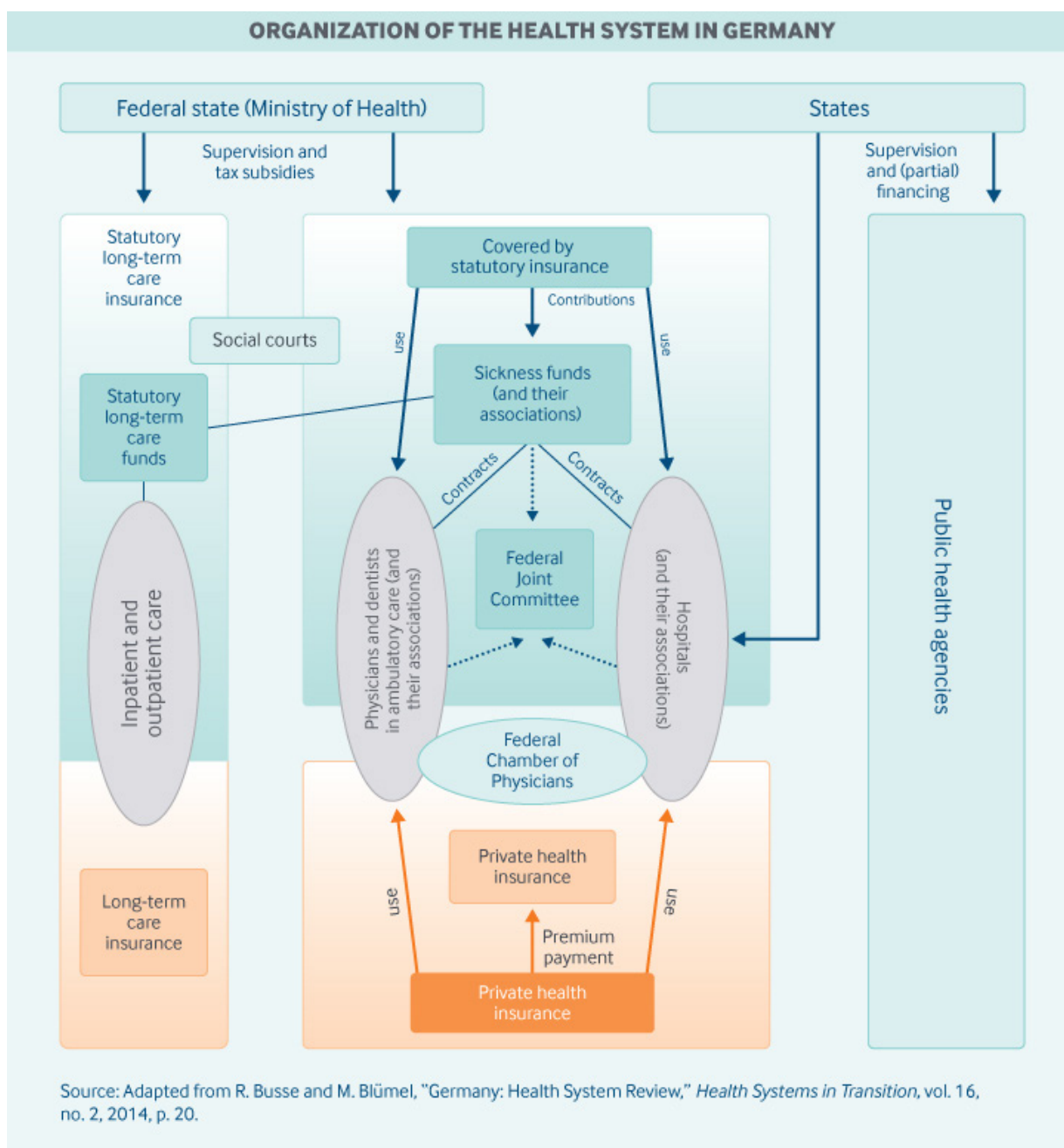
32 BUNDESGESUNDHEITSMINISTERIUM. **Das deutsche Gesundheitssystem**. Disponível em: [https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5\\_Publikationen/Gesundheit/Broschueren/200629\\_BMG\\_Das\\_deutsche\\_Gesundheitssystem\\_DE.pdf](https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Gesundheit/Broschueren/200629_BMG_Das_deutsche_Gesundheitssystem_DE.pdf). Acesso em: 09 mar. 2022.

33 COMMONWEALTH FUND. **Germany**. Disponível em: <https://www.commonwealthfund.org/international-health-policy-center/countries/germany>. Acesso em: 09 mar. 2022.



O GKV é, portanto, um componente central do sistema de saúde alemão. A estrutura do GKV tem sido reformada reiteradamente ao longo dos últimos 25 anos, com o objetivo de torná-lo mais eficiente. Os fundos de seguro de saúde foram gradualmente habilitados a assinar acordos individuais para tratamentos específicos com médicos, associações médicas e hospitais, além de empresas farmacêuticas, geralmente para fins de descontos. Após um período de reformas em diversas áreas do sistema de saúde entre 2012 e 2016, novos debates e propostas de reforma permaneceram inertes até 2018, sobretudo por questões político-partidárias. A partir de então, como se verá nos tópicos seguintes, novas iniciativas legislativas foram tomadas, visando principalmente à modernização do sistema de saúde alemão, com sua completa digitalização, inclusive com a interoperabilidade dos dados de saúde centradas no controle dos dados pelos pacientes.

A organização do sistema de saúde da Alemanha se encontra esquematizada no infográfico<sup>34</sup> abaixo:



34 Cf.: <https://www.commonwealthfund.org/international-health-policy-center/countries/germany;>

## 2.4.2 O uso de dados de saúde na Alemanha

De modo geral, o uso de dados de saúde e sistemas de informação é menos avançado na Alemanha do que em vários outros países europeus, em parte devido à complexa estrutura do sistema de saúde do país<sup>35</sup>. Embora o desenvolvimento de uma infraestrutura de telemática (TI) e a introdução de aplicativos digitais médicos remontem ao ano de 2015, com a promulgação da Lei sobre Comunicação Digital Segura e Aplicações na Saúde (*E-health Act*)<sup>36</sup>, foi somente em 2019 que o governo alemão iniciou suas ações em direção a um sistema eletrônico de saúde totalmente desenvolvido, principalmente devido à pandemia da COVID-19.

A pandemia de COVID-19 mostrou que o intercâmbio de dados entre os provedores de assistência médica e a disponibilidade de conjuntos de dados nacionais para pesquisa é essencial para um sistema de assistência médica eficiente e de rápida resposta. Os desafios particulares para a Alemanha durante a pandemia foram a lenta digitalização nos escritórios de saúde pública e os atrasos na transmissão de dados ao Instituto Robert Koch, o órgão responsável por monitorar e avaliar informações sobre casos e mortes na COVID-19. Entretanto, a introdução do Sistema Alemão de Relatórios Eletrônicos e Informações para Controle de Infecções em 2020 foi um desenvolvimento significativo, o que levou à comunicação digital dos resultados positivos dos testes de COVID-19 pelos laboratórios às autoridades sanitárias e ao Instituto Robert Koch<sup>37</sup>.

Nesse contexto, o desenvolvimento de um sistema de saúde eletrônico mais eficiente tornou-se crucial. A Lei de Saúde Digital, de 2019, estabelece a base legal para transferir dados dos fundos de saúde para um centro de dados de pesquisa e torná-los acessíveis à comunidade científica, enquanto o Acordo de Saúde Pública, assinado em 2020, visava a promover a digitalização dos serviços de saúde pública. Para reforçar a importância dessa questão política, a Alemanha colocou a digitalização e o intercâmbio seguro de dados relacionados à saúde dentro da UE na agenda de sua presidência do Conselho da UE em 2020, levando a novas iniciativas que objetivam promover um melhor intercâmbio e acesso a diferentes tipos de dados de saúde (tais como prontuários de saúde eletrônicos, dados genômicos, dados de registros de pacientes), para promover uma melhor prestação de cuidados de saúde, pesquisas em saúde e elaboração de políticas públicas.

A seguir, apresentaremos e discutiremos, em maior ou menor medida, as principais disposições das recentes legislações alemãs sobre uso de dados de saúde.

---

35 OECD. **Germany: Country Health Profile 2021**. Paris: Organisation for Economic Co-operation and Development, 2021. Disponível em: <https://www.oecd-ilibrary.org/docserver/e4c56532-en.pdf?expires=1646001678&id=id&accname=guest&checksum=360F309A62325931855ECACB6AE85E2E>. Acesso em: 03 mar. 2022.

36 BUNDESGESUNDHEITSMINISTERIUM. **Das E-health-Gesetz**. Disponível em: <https://www.bundesgesundheitsministerium.de/service/begriffe-von-a-z/e/e-health-gesetz.html>. Acesso em: 4 mar. 2022.

37 OECD. **Germany: Country Health Profile 2021**. Paris: Organisation for Economic Co-operation and Development, 2021. Disponível em: <https://www.oecd-ilibrary.org/docserver/e4c56532-en.pdf?expires=1646001678&id=id&accname=guest&checksum=360F309A62325931855ECACB6AE85E2E>. Acesso em: 03 mar. 2022.

### 2.4.2.1 Proteção dos Dados do Paciente (Patientendaten-Schutz-Gesetz – PDSG) – 2020

Em 3 de julho de 2020, o Parlamento Federal da Alemanha, o Bundestag, aprovou a Lei de Proteção de Dados dos Pacientes ou Patientendaten-Schutz-Gesetz (PDSG). A PDSG é parte de um esforço para a digitalização do sistema de saúde alemão, introduzindo uma série de iniciativas digitais inovadoras, além de requisitos para a proteção das informações dos pacientes armazenadas em formato eletrônico (como se verá a seguir). Trata-se de lei que, seguindo a forte tradição alemã em proteção de dados, centra o controle de acesso no próprio paciente, titular dos dados, que tem a prerrogativa inclusive de indicar qual tipo de profissional de saúde pode ter acesso a qual tipo de dado, fazendo com que o consentimento do titular seja determinante não só para usos secundários, como também para os usos primários.

A primeira versão da lei foi fortemente criticada pelo Comissário Federal de Proteção de Dados e Liberdade de Informação (*Bundesbeauftragte für den Datenschutz und die Informationsfreiheit – BfDI*), órgão com atuação semelhante à da Autoridade Nacional de Proteção de Dados brasileira. Com efeito, na versão inicial da lei, os dados de saúde contidos no prontuário médico compartilhado eram visíveis para toda a equipe de saúde, de modo que um dentista, por exemplo, poderia ter acesso aos relatórios médicos de um paciente submetidos por um psiquiatra. Na versão final da lei, o legislador alemão esclareceu, em consonância com as disposições do GDPR, que o paciente permaneceria no controle de seus dados de saúde e poderia decidir quais dados ele desejava compartilhar ou excluir. Além disso, o paciente deverá decidir sozinho sobre o uso do prontuário médico compartilhado.

Vale ressaltar que a PDSG se aplica a todas as instituições de saúde, incluindo hospitais, médicos, provedores de seguros de saúde e farmácias que utilizam serviços, aplicativos e componentes da infraestrutura telemática do sistema de saúde alemão para processar informações aos pacientes, não importando o tamanho da instituição.

Com a PDSG, a partir de 2021 os fornecedores de seguros de saúde foram obrigados a oferecer aos clientes os seus “registros eletrônicos” – *elektronische Patientenakte* (ePA). A partir de 2022, os ePAs também incluirão informações sensíveis que até então só eram registradas em papel, tais como registros de maternidade, registros de saúde pediátrica e carteiras de vacinação. Os pacientes terão o poder de decidir o que será armazenado em seus ePAs e quem terá acesso a eles. O uso do ePA é voluntário, mas o governo alemão ressaltou que o paciente é quem terá o poder de decidir sobre o que acontece com seus dados, tornando-se “mestre de seus dados pessoais”<sup>38</sup>.

A partir de 2022, os segurados também poderão usar seu smartphone ou *tablet* para determinar quem pode acessar cada documento armazenado no ePA. Por exemplo, os pacientes podem especificar que um médico pode acessar os registros médicos eletrônicos, mas que certas informações não são exibidas para ele. E, a partir de 2023, os pacientes poderão, voluntariamente, disponibilizar dados sobre seus ePAs a pesquisadores, em

---

38 BUNDESGESUNDHEITSMINISTERIUM. **Patientendaten-Schutz-Gesetz**. Disponível em: <<https://www.bundesgesundheitsministerium.de/patientendaten-schutz-gesetz.html>>. Acesso em: 4 mar. 2022.

uma espécie de “doação” de dados. Os pacientes precisarão dar seu consentimento livre e esclarecido para a doação, poderão fazê-lo digitalmente. Os pacientes também poderão escolher o escopo de sua doação de dados e limitar o acesso a certas informações.

Com a PSDG, médicos deverão fornecer prescrições eletrônicas aos pacientes, que deverão ser assinadas digitalmente e inseridas no sistema de IT desenvolvido pelo governo. Os pacientes poderão acessar a receita eletrônica a partir de seu smartphone, usando um aplicativo, e enviá-la a uma farmácia de sua escolha. As farmácias poderão então acessar a receita eletrônica a partir do sistema telemático e introduzi-la no sistema de administração da farmácia para liberar a receita. Embora os pacientes ainda possam optar por receber uma receita em papel de seu médico, ela ainda deverá ser registrada no sistema e recuperada digitalmente pela farmácia usando as informações fornecidas na receita em papel.

Todas essas inovações evidentemente despertam preocupações quanto à proteção dos dados pessoais dos pacientes. Nesse sentido, a PSDG estabelece que, a partir de 1º de janeiro de 2022, todas as instituições de saúde, independentemente de seu tamanho, deverão tomar precauções para evitar qualquer risco à disponibilidade, integridade e confidencialidade dos dados dos pacientes que processam no sistema telemático. Também serão obrigadas a proteger seus sistemas tecnológicos, componentes e processos cruciais para proteger as informações dos pacientes e a funcionalidade da rede do hospital. Por serem pontos de acesso à infraestrutura telemática, os sistemas de computador das instituições de saúde devem ser protegidos, o que significa tanto aplicar medidas básicas de segurança cibernética, como firewalls, software antivírus e políticas de senha fortes, como também garantir que os dados sensíveis não sejam armazenados localmente quando não houver necessidade deles ou que sejam transferidos através de canais não autorizados, como e-mails ou compartilhamento de arquivos e serviços em nuvem. O BfDI também advertiu os prestadores de seguro de saúde que estão sob sua jurisdição que o cumprimento da PSDG não os isentará da necessidade de cumprir com as demais disposições do Regulamento Geral de Proteção de Dados (GDPR) europeu<sup>39</sup>.

### **2.4.3 Digitalização e Interoperabilidade de dados de saúde na Alemanha**

#### **2.4.3.1 Lei de Saúde Eletrônica (E-health Act) – 2015**

A “Lei sobre Comunicação Digital Segura e Aplicativos em Saúde (*E-health Act*)”, que entrou em vigor em 29 de dezembro de 2015, estabeleceu o curso para o desenvolvimento de uma infraestrutura de telemática (TI) segura e a introdução de aplicativos digitais médicos. O objetivo da lei é utilizar as oportunidades de digitalização para a saúde e permitir a rápida introdução de aplicativos médicos para os pacientes.

O foco da regulamentação diz respeito, principalmente: à criação de incentivos para a rápida introdução e utilização de aplicativos médicos (gerenciamento de dados dos segurados/usuários, receituário eletrônico e plano de medicação uniforme); criação de uma infraestrutura de telemática e à perspectiva de desenvolvimento em direção a uma infra-

---

39 BUNDESGESUNDHEITSMINISTERIUM. *Patientendaten-Schutz-Gesetz*. Disponível em: <<https://www.bundesgesundheitsministerium.de/patientendaten-schutz-gesetz.html>>. Acesso em: 4 mar. 2022.

estrutura definitiva e segura para o sistema de saúde alemão; criação de um diretório de interoperabilidade para melhorar a comunicação de diferentes sistemas de TI no setor de saúde; e ao fomento a serviços de telemedicina<sup>40</sup>.

Embora consideradas visionárias à época, muitas de suas disposições não eram suficientemente abrangentes para ter um impacto significativo. Por exemplo, a lei instituiu o registro eletrônico de pacientes que não contava com o histórico de seus dados médicos, bem como uma infraestrutura de intercâmbio de dados telemáticos para profissionais de saúde que englobava médicos e demais profissionais da área, mas não incluía hospitais e farmácias. Além disso, a Lei de Saúde Eletrônica não cobriu tópicos importantes como receitas médicas eletrônicas (e-prescrições) e telemedicina. No entanto, a lei foi fundamental para provocar o debate político sobre a digitalização dos serviços de saúde na Alemanha, servindo de base para novas leis que seriam promulgadas nos anos seguintes<sup>41</sup>.

#### 2.4.3.2. Lei de Saúde Digital (Digitale-Versorgung-Gesetz – DVG) – 2019

A “Lei para melhoria da prestação de serviços de saúde através da digitalização e inovação” (*Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation*, também conhecida por *Digitale-Versorgung-Gesetz*, ou simplesmente DVG) foi aprovada em 7 de novembro de 2019 pelo *Bundestag* e adotada em 29 de novembro de 2019 pelo *Bundesrat*. Trata-se de uma lei ambiciosa destinada a catalisar a transformação digital do sistema de saúde alemão, que historicamente tem se mostrado atrasado nessa área entre os países europeus<sup>42</sup>.

Em se tratando de inovação tecnológica, algumas das disposições mais importantes da DVG são a formalização de “aplicativos prescritíveis” (*Digitale Gesundheitsanwendungen*, ou DiGA) – que incluem softwares padrão, SaaS (*software as a service*) e aplicativos móveis – e a criação do Processo *Fast-Track*, um caminho regulatório acelerado para que empresas lancem seus aplicativos de saúde digital no mercado – após uma revisão simplificada, um aplicativo pode ser adicionado a um registro central de aplicativos<sup>43</sup>, e poderá

40 BUNDESGESUNDHEITSMINISTERIUM. *Das E-health-Gesetz*. Disponível em: <https://www.bundesgesundheitsministerium.de/service/begriffe-von-a-z/e/e-health-gesetz.html>. Acesso em: 4 mar. 2022.

41 Além das leis tratadas neste documento, o *E-health Act* serviu de base para a instituição do Service Supply Act, (2) Drug Safety and Supply Act, and (3) Digital Provision Act.

42 STERN, A. D. et al. Want to See the Future of Digital Health Tools? Look to Germany. **Harvard Business Review**, 2 dez. 2020.

43 O Processo *Fast-Track* é administrado pelo Instituto Federal de Medicamentos e Dispositivos Médicos (*Bundesinstitut für Arzneimittel und Medizinprodukte*, ou BfArM), que desempenha muitas das mesmas funções na Alemanha que a Anvisa desempenha no Brasil. O BfArM também mantém o registro dos *DiGA*. Os cinco primeiros aplicativos já foram adicionados ao registro e oferecem apoio aos pacientes para cuidar de condições que incluem zumbido, obesidade, agorafobia, osteoartrose e insônia.

Para ser listado e permanecer no registro dos *DiGA* e qualificar-se para reembolso pelas seguradoras de saúde, um aplicativo deve preencher vários requisitos. Estes incluem proteção de dados, segurança da informação, interoperabilidade e dados preliminares sobre os benefícios que o aplicativo proporciona. Após o exame de segurança, funcionalidade, qualidade, segurança de dados e proteção de dados pelo Instituto Federal de Medicamentos e Dispositivos Médicos (BfArM), o aplicativo será provisoriamente reembolsado pelo seguro de saúde obrigatório pelo período de um ano. Durante esse período, os fabricantes devem provar ao Institu-

ser prescrito por médicos e psicoterapeutas, sendo reembolsável por todos os provedores de seguros de saúde públicos da Alemanha<sup>44</sup>, que abrangem 90% da população, ou aproximadamente 73 milhões de indivíduos. Os pacientes poderão, portanto, utilizar os aplicativos de cuidados em saúde de maneira mais abrangente e eficaz, uma vez que os médicos poderão prescrever esses aplicativos, e os seguros de saúde públicos irão pagar por eles, ou reembolsar os pacientes pelo seu uso<sup>45</sup>.

Outra inovação é a criação de uma rede digital obrigatória para o setor da saúde. Os pacientes podem usar produtos digitais como o prontuário eletrônico do paciente em todo o país. Farmácias e hospitais foram obrigados a filiar-se à infraestrutura telemática desenvolvida pelo governo. Parteiras e fisioterapeutas, assim como instalações de cuidados de longo prazo e de reabilitação podem se filiar à TI de forma voluntária, e os custos incorridos para a filiação voluntária serão reembolsados. Os médicos que se recusarem a se conectar estão sujeitos a penalidades de ordem econômica.

Além do prontuário eletrônico, outros documentos poderão ser emitidos eletronicamente. O atestado médico, a prescrição de remédios (*e-prescription*) e todos os outros benefícios previstos, tais como medicamentos e dispositivos de assistência ou serviços de enfermagem domiciliar, podem ser prescritos eletronicamente. Outra inovação é a previsão de reembolso para consultas realizadas por videochamada, o que vai ao encontro das iniciativas de fomento à telemedicina no país.

Importante destacar que a integração de bases de dados médicas no país é realizada não pela centralização, mas pela instituição de interfaces abertas e padronizadas para compartilhamento de informação, que serão desenvolvidas com base em padrões internacionais.

#### **2.4.3.3 Lei de Modernização da Assistência Digital à Saúde (*Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz*) - 2021**

Em 6 de maio, o Bundestag aprovou a Lei de Modernização da Assistência Digital à Saúde (*Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz*), com o objetivo de ele-

to Federal que seu aplicativo contribui para melhorar a saúde dos pacientes. Os fabricantes negociam então a quantia que receberão pelo aplicativo com a Associação Federal Central dos Fundos de Seguro de Saúde (*GKV-Spitzenverband*).

44 O seguro de saúde é obrigatório na Alemanha. A grande maioria da população alemã (90%) recebe cobertura do seguro de saúde estatal (*Gesetzliche Krankenversicherung*). Os outros 10% estão cobertos por seguros privados (*Privat Krankenversicherung*).

45 Antes do DVG, o uso de aplicativos ou outros softwares médicos oferecidos aos pacientes só poderia ser reembolsado por uma seguradora com base em uma análise caso a caso ou com base em acordos seletivos especiais. O primeiro processo era muito complexo para o paciente e não oferecia um modelo de negócio sustentável para o fornecedor do aplicativo ou software. Um acordo seletivo era e é uma forma de ter o produto reembolsado pelas seguradoras de saúde estatais, mas estes acordos eram limitados temporalmente e não permitiam uma cobertura de mercado abrangente na Alemanha. Uma vez que o contrato caducasse, não havia um caminho direto para o reembolso. Com o DVG, os aplicativos digitais de saúde podem ser mais facilmente reembolsados por fundos de seguro de saúde estatutários, tornando-os mais acessíveis aos pacientes.

var o potencial dos dados de saúde<sup>46</sup> para melhoria do setor. A lei marca o próximo passo da digitalização do sistema de saúde legal alemão, que já conta com a Lei de Saúde Digital (*Digitale-Versorgung-Gesetz*) e a Lei de Proteção de Dados dos Pacientes (*Patientendaten-Schutz-Gesetz*), abordadas nos itens anteriores.

De acordo com a nova lei, partir de 1º de janeiro de 2023, os fundos de seguro de saúde deverão fornecer aos segurados uma identidade digital segura e “sem barreiras” dentro do sistema de saúde, que poderá ser solicitada mediante requerimento, além do cartão eletrônico de saúde (*elektronische Gesundheitskarte*). Essas identidades digitais têm o objetivo de autenticar o segurado dentro do sistema de saúde (como em consultas em vídeo) e como prova de titularidade do seguro, de forma semelhante ao cartão eletrônico de saúde. A lei estabelece ainda que a identidade digital poderá adotar uma variedade de formas, apresentando diferentes níveis de segurança e confidencialidade.

Até julho de 2022, os fundos de seguro de saúde devem disponibilizar procedimentos para usuários autorizados testarem a integração da identidade digital. A *Gematik* (órgão de certificação governamental para assuntos de saúde digital da Alemanha) deverá criar a base técnica para introdução da funcionalidade até abril de 2022.

Futuramente, os dados relativos ao fornecimento de medicamentos, até então armazenados no cartão eletrônico de saúde, serão acessados no aplicativo correspondente dentro do sistema de TI do governo alemão. Os segurados poderão retirar medicamentos em farmácias apenas com a prova de sua identidade, e espera-se que essa funcionalidade seja estendida para demais países europeus.

Será desenvolvido também uma espécie de “resumo eletrônico” do paciente, em que os dados dos pacientes necessários para fins de emergência serão armazenados e tornados disponíveis de maneira mais simples, facilitando a comunicação com membros da família ou profissionais de saúde.

Além disso, algumas funcionalidades devem ser acrescentadas aos procedimentos de transmissão de informações, a partir do serviço de TI denominando KIM (*Kommunikation im Medizinwesen*, “Comunicação em Medicina”), que irá permitir a comunicação entre segurados, prestadores de serviços de saúde e terceiros pagadores, com a implementação das restrições de acesso para cada ator desde a concepção. Além da função de e-mail, os procedimentos de comunicação também permitirão o serviço de comunicação por vídeo e oferecerão um serviço de mensagens.

Outro ponto importante para médicos e outros prestadores de serviço de saúde no que diz respeito aos deveres de *accountability* referente ao tratamento dos dados pessoais dos pacientes é a necessidade de realização de avaliações de impacto de proteção de dados.

Com a nova Lei, espera-se que novos aplicativos digitais para saúde sejam desenvolvidos, tanto para fins de cuidado quanto para prevenção de doenças e condições médicas (o pró-

---

46 BUNDESGESUNDHEITSMINISTERIUM. *Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz*. Disponível em: <<https://www.bundesgesundheitsministerium.de/service/gesetze-und-verordnungen/guv-19-lp/dvpmg.html>>. Acesso em: 4 mar. 2022.

prio governo alemão dá o exemplo de aplicativos para exercícios que diminuem o risco de quedas, ou auxiliem no fortalecimento da memória de pacientes com demência). Será criado um procedimento para verificar a elegibilidade de reembolso dos aplicativos de saúde digitais e para inclusão desses aplicativos no repositório do BfArM. Ademais, os segurados terão a possibilidade de inserir os dados de seus aplicativos de saúde diretamente em seu arquivo eletrônico de paciente, e os serviços prestados por fornecedores de medicamentos e parceiras em conexão com os aplicativos serão remunerados no futuro.

Os serviços de telemedicina também estão sendo expandidos. Será criado um portal único para oferecimento de serviços de telemedicina, tanto em formato de sítio eletrônico quanto via telefone, de modo que o paciente não precisará mais entrar em contato com o profissional de saúde diretamente.

Por fim, vale mencionar a expansão da infraestrutura de telemática, tanto a nível nacional quanto relativo ao bloco. No âmbito do *Gematik*, estão sendo estudados pré-requisitos para o desenvolvimento do diretório de interoperabilidade, que deverá ser convertido em uma plataforma de conhecimento e em um novo centro de interoperabilidade dentro do sistema de saúde alemão. Serão estabelecidas diretrizes de padronização dos serviços e aplicativos digitais em saúde, além do desenvolvimento de recomendações para o uso dos dados. E a fim de fortalecer a segurança dos pacientes que utilizam serviços de saúde em outros países da União Europeia, pretende-se criar, até o meio de 2023, um ponto de contato nacional para *e-health*, que permitirá que pacientes alemães possam fornecer seus dados médicos a profissionais da saúde em outros países europeus de maneira segura e com tradução.

Embora tenha ingressado tardiamente na “corrida” pela digitalização, a Alemanha tem ampliado significativamente as bases para vasta gama de inovações digitais, visando padronizar e modernizar o sistema de saúde alemão nos próximos anos. Resumidamente, as inovações dizem respeito à obrigatoriedade de inserção dos profissionais de saúde, bem como hospitais e farmácias, no sistema de infraestrutura telemática governamental, além do fortalecimento da telemedicina e ao incentivo a aplicativos de saúde, principalmente no que se refere à sua regulamentação. O ponto central das inovações, todavia, é a autodeterminação do paciente, que deverá ter controle sobre o acesso aos seus dados pessoais e sobre o compartilhamento destes em uma infraestrutura informática interoperável.

## 2.5 Itália

### 2.5.1 Organização do sistema de saúde<sup>47</sup> italiano

O Serviço Nacional de Saúde da Itália é descentralizado e de base regional. O governo central canaliza a receita tributária geral para a assistência médica financiada publicamente, define o pacote de benefícios e exerce a administração geral. Cada região é responsável pela organização e prestação de serviços de saúde através de unidades de saúde locais e através de hospitais públicos e privados credenciados.

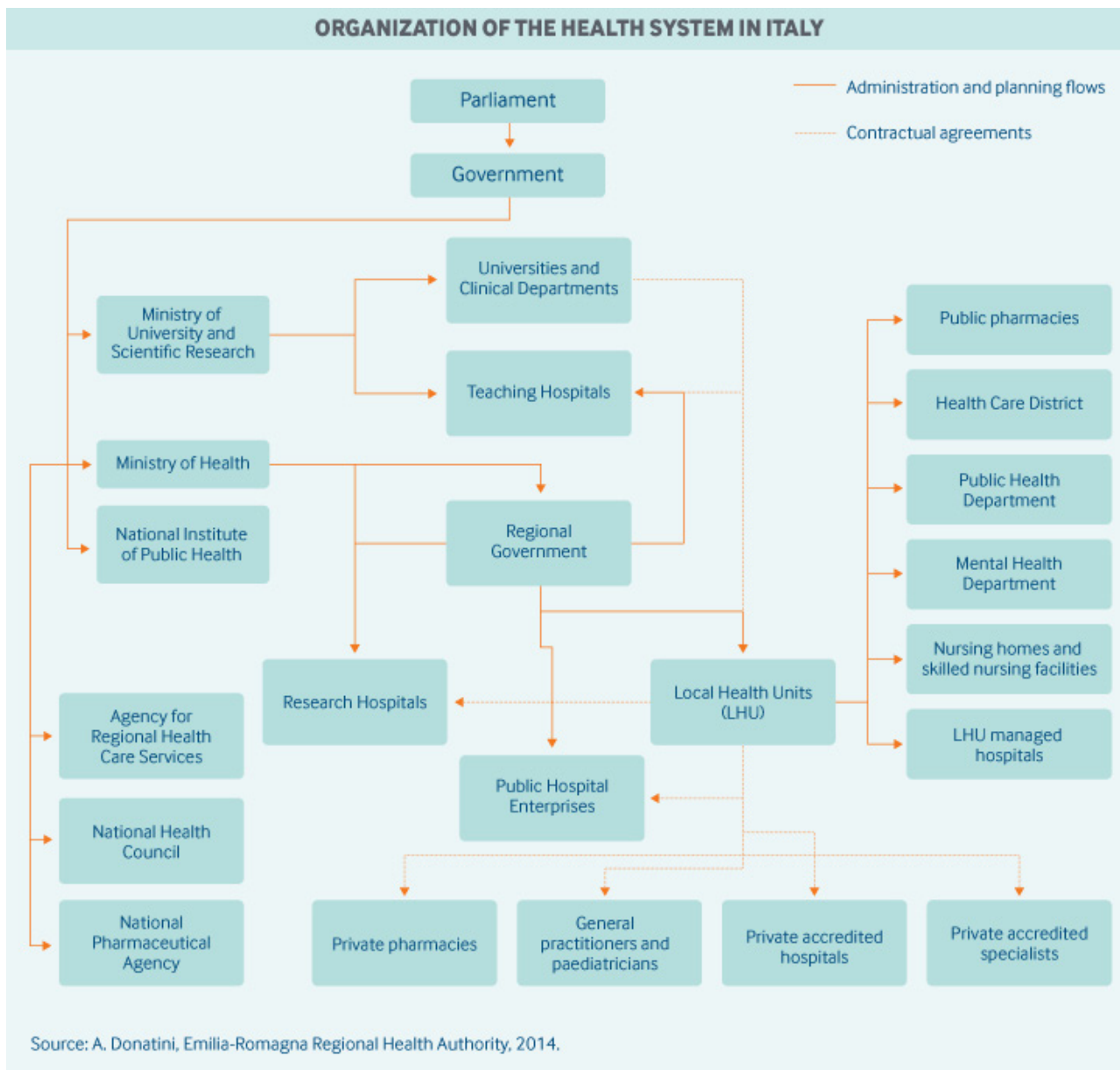
---

47 Cf.: <https://www.oecd-ilibrary.org/docserver/5bb1946e-en.pdf?expires=1644661801&id=id&accname=guest&checksum=537EEE6BEC5CA3AB77849C0DB185D683>



Em 2019, a Itália gastou 8,7% do PIB com a saúde, em comparação com a média da UE de 9,9%. No mesmo ano, os gastos per capita atingiram 2 525 euros (ajustados pelas diferenças de poder de compra), o que está mais de 25% abaixo da média da UE (3 523 euros). Historicamente, os gastos com saúde na Itália sempre foram inferiores à média da UE, mas nos últimos cinco anos ocorreram aumentos lentos, impulsionados principalmente por um crescimento dos gastos privados. O gasto público como proporção do gasto total com saúde foi de 74% em 2019 - menor do que a média da UE de 80%. A maior parte das despesas restantes veio de despesas extras pelas famílias (23%), já que o seguro voluntário de saúde (VHI) desempenha apenas um papel menor (cobrindo apenas 3% do total).

O infográfico<sup>48</sup> abaixo ilustra o funcionamento do sistema de saúde italiano:



## 2.5.2 O sistema italiano de dados de saúde

As leis 179/2012 e 98/2013, bem como o Decreto n. 178/2015 fornecem o arcabouço legal para a definição do Registro Eletrônico de Saúde (EHR), que cada região italiana e província autônoma deve estabelecer através de uma infraestrutura tecnológica capaz de

48 Cf.: <https://www.commonwealthfund.org/international-health-policy-center/countries>

interagir com as outras soluções regionais de EHR, expondo serviços apropriados que permitam a realização de uma série de processos inter-regionais. Isso porque, na Itália, a autonomia sobre a saúde proporcionada pela Constituição a cada região levou à disseminação de sistemas regionais muito heterogêneos, com dificuldade de interoperar.

Os serviços de interoperabilidade permitem realizar a busca, recuperação, registro, cancelamento de documentos. As mudanças regulamentares ocorridas no contexto da Lei do Orçamento de 2017 (Lei 11 de dezembro de 2016, no.232 publicada no Diário Oficial no.297 de 21 de dezembro de 2016) introduziram a Infraestrutura Nacional de Interoperabilidade (INI), cujo projeto é da Agência para a Itália Digital, em acordo com o Ministério da Saúde e o Ministério da Economia e Finanças e com as regiões e províncias autônomas, e cuja implementação é fornecida pelo Ministério da Economia e Finanças. O INI tem a tarefa de assegurar a interoperabilidade dos EHR regionais, a identificação da pessoa assistida através do alinhamento com o Registro Nacional de Pacientes.

Os processos de interoperabilidade, funcionalidades, métodos de acesso e regras técnicas de interação entre os sistemas regionais e o INI estão descritos na circular da AgID no. 4/2017 de 1 de agosto de 2017, no Decreto Ministerial de 4 de agosto de 2017 do Ministério da Economia e Finanças, em acordo com o Ministério da Saúde e nas especificações técnicas relacionadas. Estes documentos foram produzidos como parte de um grupo de trabalho no qual participaram ativamente a Agência para a Itália Digital, o Ministério da Saúde, o Ministério da Economia e Finanças, a Autoridade Italiana de Proteção de Dados, as regiões italianas e as províncias autônomas, Sogei e o Conselho Nacional de Pesquisa da Itália.<sup>49</sup>

De acordo com as normas indicadas acima, o EHR pode ser usado para três finalidades: a) prevenção, diagnóstico, tratamento e reabilitação; b) estudo e pesquisa científica no campo médico, biomédico e epidemiológico; c) planejamento de saúde, verificação da qualidade do atendimento e avaliação do atendimento de saúde. Ou seja, não é permitido o compartilhamento do EHR com entidades responsáveis pela gestão de pagamento e reembolso ou seguros de saúde. Com relação aos usos para planejamento e pesquisa valem os princípios de *privacy by design e by default* com o uso mínimo e técnicas de pseudonimização ou anonimização com a agregação de informações para a construção de políticas públicas de saúde.

O marco regulatório permitiu a um Conselho Técnico Nacional definir um conjunto de diretrizes de referência para a implementação dos sistemas EHR. Em seguida, um conjunto de especificações técnicas, que estabelecem os principais requisitos a serem atendidos pelas regiões, foi definido para garantir a interoperabilidade em diferentes níveis: a interoperabilidade técnica é assegurada pelo compartilhamento de protocolos de comunicação entre interfaces de serviços; a interoperabilidade sintática é alcançada pelo uso de formatos de dados comuns; a interoperabilidade semântica é garantida pela adoção dos mesmos formatos de dados e sistemas de codificação; a interoperabilidade de organizações e serviços é possibilitada pelo compartilhamento de processos transfronteiriços comuns.

---

49 Cf.: <https://www.fascicolosanitario.gov.it/en/EHRs-Interoperability>

Cada sistema regional EHR está sendo desenvolvido de acordo com os requisitos especificados pela norma, diretrizes e especificações. As principais restrições arquitetônicas impostas são as seguintes:<sup>50</sup>

- i) Consentimento do paciente: cada paciente pode tirar proveito das funcionalidades oferecidas pelo sistema EHR da região do prestador de serviços de saúde do paciente. Para este objetivo, ela/ele tem que expressar dois tipos de consentimento: i) um consentimento que permita a constituição do EHR com seus documentos clínicos pelas instalações de saúde; ii) um consentimento que permita a consulta do EHR pelos profissionais de saúde. Especificamente, é permitido ao paciente escolher as funções profissionais permitidas para acessar seu EHR, definindo políticas específicas de privacidade.
- ii) Modelo de Metadados de Índice: a região do provedor de saúde do paciente tem a responsabilidade de manter metadados de índice relacionados a todos os documentos relacionados a seus pacientes, mesmo que tais documentos sejam produzidos e mantidos por unidades de saúde localizadas fora da região.
- iii) Modelo de Interoperabilidade baseado em Proxy: o sistema da região provedora de serviços de saúde tem que operar como um mediador com os outros sistemas regionais em todos os processos transfronteiriços nos quais seus pacientes estão envolvidos.

### 2.5.3 Seguro saúde e dados pessoais na Itália

Como não é permitido que as pessoas optem por sair do sistema e busquem apenas cuidados privados, não existe um seguro substitutivo. Os seguros de saúde complementares e suplementares privados desempenham um papel limitado no sistema de saúde, representando cerca de 1% do total de gastos em 2014 na Itália.

Aproximadamente 10% da população tem alguma forma de seguro de saúde voluntário, que cobre serviços excluídos sob os benefícios essenciais do sistema de saúde, oferece um padrão mais alto de conforto e privacidade nas instalações hospitalares e oferece uma escolha mais ampla entre os provedores públicos e privados. Algumas apólices de seguro de saúde privado também cobrem copagamentos para serviços privados ou uma taxa diária de compensação durante a hospitalização. Benefícios fiscais favorecem o seguro complementar (seguro para copagamentos) sobre o seguro voluntário suplementar (que cobre o custo dos serviços de saúde não incluídos no pacote de benefícios essenciais).

Como não há regras específicas autorizando o compartilhamento de dados com seguradoras privadas, o compartilhamento deve seguir as diretrizes da legislação de proteção de dados, tendo, como principais bases legais de tratamento, o consentimento do titular e os atos necessários para a execução de cláusulas contratuais.

---

50 Cf.: <https://www.scitepress.org/papers/2016/59164/59164.pdf>

## 2.6 Conclusões parciais sobre países da Comunidade Europeia

A análise dos sistemas de saúde, proteção de dados e implantação de operabilidade e modelos de *e-health* nos países europeus selecionados, que são representativos do modelo em geral adotado na Comunidade Europeia, permite destacar alguns pontos interessantes:

- i) O sistema de saúde dos países Europeus é fortemente baseado em recursos públicos, com os serviços fornecidos em estabelecimentos públicos de saúde, muito embora haja um mercado crescente de saúde suplementar baseado no financiamento e contratação privada pelos beneficiários;
- ii) O atendimento à saúde é, em geral, descentralizado, sendo prestado em escalas estadual ou local e coordenados por sistema e legislações nacionais;
- iii) Os países europeus têm investido significativamente na digitalização do atendimento à saúde, em particular em prontuários eletrônicos e na interoperabilidade dos sistemas empregados nos diferentes estabelecimentos de saúde;
- iv) A proteção de dados pessoais é pilar fundamental na implantação da digitalização e interoperabilidade dos sistemas, sendo que os diferentes países seguem, além da GDPR, legislação local especificando restrições ao acesso e compartilhamento de dados constantes em prontuários eletrônicos;
- v) Em geral, a interoperabilidade, independentemente de consentimento, restringe-se ao uso primário, ou seja, ao acesso pelos médicos e estabelecimentos de saúde, no contexto de prestação de atenção e cuidado em relação ao paciente, tendo como base legal (autorizadora do tratamento) principalmente o cumprimento de obrigação legal;
- vi) A interoperabilidade se dá não pela centralização dos dados em esfera federal, mas pelo estabelecimento de padrões técnicos nacionais a serem observados para que os diferentes sistemas permitam, entre si, o acesso e compreensão dos dados de saúde, em particular, dos prontuários médicos;
- vii) Trata-se, portanto, de interoperabilidade de dados, implantada por meio do acesso a pessoas autorizadas, que se restringem aos profissionais de saúde e estabelecimentos de saúde (hospitais e clínicas, particulares ou privados);
- viii) Na Alemanha, país com forte tradição em proteção de dados, inclusive adota-se modelo fortemente apoiado no princípio de autonomia informacional do paciente, em contexto de estímulo a criação de sistemas e aplicativos de saúde interoperáveis, de modo que o próprio paciente tem a prerrogativa de determinar quem acessa quais tipos de informação de saúde, o que pode inclusive limitar o acesso de profissionais de saúde e estabelecimentos de saúde a determinados tipos de informação, caso não haja relação direta com o escopo do tratamento médico;
- ix) O uso secundário de dados de prontuários eletrônicos para a finalidade de pesquisa ou formulação de políticas públicas de saúde depende de previsão em lei ou deve se basear no consentimento do titular do dado, devendo ainda adotar as medidas necessárias, caso possível, para a desidentificação dos pacientes;

- x) O uso secundário para gestão do pagamento aos estabelecimentos e profissionais de saúde tem que ser analisado com base no princípio de proporcionalidade e necessidade, ou seja, o tratamento e acesso a dados deve se limitar ao necessário para a realização dos reembolsos. Inexistindo previsão legal expressa, ou não sendo necessário o tratamento para execução do objeto do contrato de seguro, o envio de dados de saúde deve estar baseado no consentimento do beneficiário.

## 2.7 Inglaterra

### 2.7.1 O sistema de saúde inglês

O Reino Unido oferece saúde pública a todos os residentes permanentes, cerca de 58 milhões de pessoas. A cobertura de saúde é gratuita em caso de necessidade, e é paga por impostos gerais. Cerca de 18% do imposto de renda de um cidadão vai para a saúde, o que representa cerca de 4,5% da renda média do cidadão. No total, cerca de 8,4% do produto interno bruto do Reino Unido é gasto com saúde (uma quantia de cerca de 0,18984 trilhões de libras esterlinas). O Reino Unido também tem um setor privado de saúde em crescimento, mas que ainda é muito menor do que o setor público.

Desde os anos 80, o total das despesas com saúde como porcentagem do PIB tem, em geral, apresentado uma tendência crescente. Além disso, o setor privado de seguros de saúde assumiu um papel mais proeminente, representando cerca de 16,7% dos gastos com saúde em 1999, contra 10,6% em 1980. Aproximadamente 10,5% da população do Reino Unido possui seguro complementar voluntário para obter acesso mais rápido aos cuidados eletivos.

A cobertura sanitária na Inglaterra tem sido universal desde a criação do Serviço Nacional de Saúde (NHS)<sup>51</sup>, em 1948. O NHS foi criado sob a Lei do Serviço Nacional de Saúde de 1946, com base nas recomendações de um relatório ao Parlamento de Sir William Beveridge em 1942. O Relatório Beveridge delineou a assistência médica gratuita como um aspecto de uma reforma mais ampla do bem-estar social, destinada a eliminar o desemprego, a pobreza e as doenças, e a melhorar a educação. Nos termos da Lei de 1946, o Ministro da Saúde tinha o dever de fornecer um serviço de saúde abrangente e gratuito, substituindo o seguro voluntário e os pagamentos feitos em dinheiro.<sup>52</sup>

Nos anos 90, o governo britânico implementou uma das mudanças mais significativas para o NHS nos últimos tempos, criando o chamado mercado interno, uma iniciativa que, grosso modo, aplicou princípios comerciais à administração pública de saúde, estimulando a "competição" entre instituições de saúde pública nos moldes da iniciativa privada. Os médicos deveriam aderir a esse mercado interno (que mais tarde viria a ser chamado

---

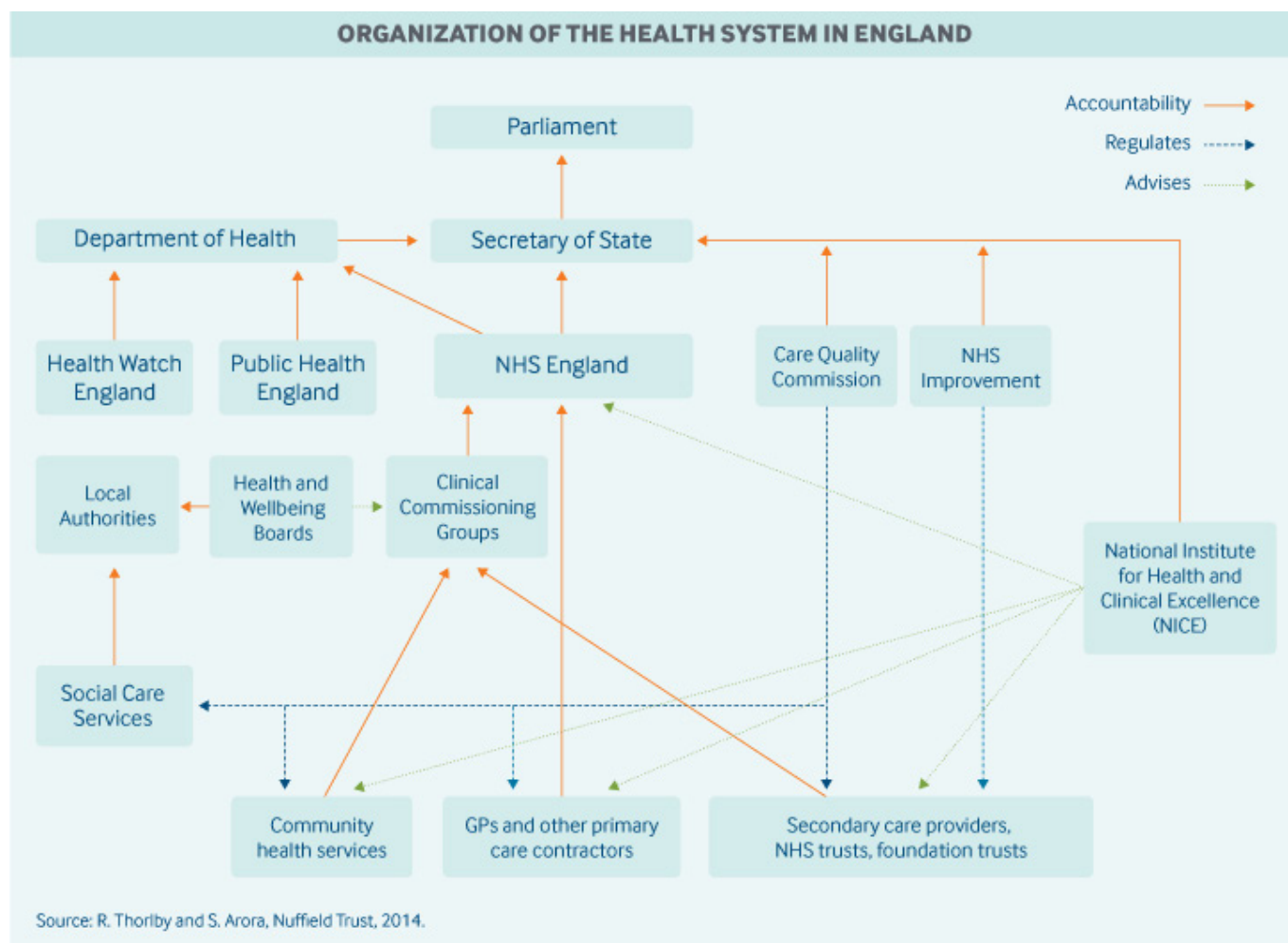
51 The NHS consists of multiple publicly funded health care systems in the United Kingdom including the NHS England, NHS Scotland, NHS Wales and Health and Social Care in Northern Ireland. Although all systems are collectively known as the NHS

52 <https://www.commonwealthfund.org/international-health-policy-center/countries/england>

NHS Trust) para poder competir pelos pacientes. Estes mercados eram organizações independentes gerenciadas individualmente e concorrentes entre si. Começou com 57 trusts e em meados dos anos 90 todos os serviços de saúde no Reino Unido eram prestados através destes trusts. Em 1998, o Reino Unido instituiu um plano de modernização, chamado de Plano NHS. O sistema carecia de padrões nacionais; faltavam incentivos e meios para melhorar o desempenho e era excessivamente centralizado nos prestadores, tirando o poder do paciente.<sup>53</sup>

A responsabilidade pela legislação e política geral de saúde na Inglaterra cabe ao Parlamento, ao Secretário de Estado da Saúde e ao Departamento de Saúde. A responsabilidade cotidiana pelo NHS é do NHS England, um órgão financiado pelo governo, que funciona separadamente do Departamento de Saúde.

A organização do sistema de saúde da Inglaterra se encontra esquematizada no infográfico<sup>54</sup> abaixo:



53 Josh Chang, Felix Peysakhovich, Weimin Wang, and Jin Zhu, *The UK Health Care System* (New York: Columbia University, 2015), accessed August 16, 2016, <http://assets.ce.columbia.edu/pdf/actu/actu-uk.pdf>, 2.

54 Cf.: <https://www.commonwealthfund.org/international-health-policy-center/countries/england>

## 2.7.2 Proteção de dados de saúde na Inglaterra

Para se preparar para o Brexit, o governo britânico adotou o *European Union (Withdrawal) Act* de 2018, que incorpora os regulamentos da UE ao direito interno. O Regulamento Geral de Proteção de Dados (GDPR) europeu foi incluído na legislação doméstica do Reino Unido até o final do período de transição do Brexit em 31 de dezembro de 2020. Após este período, o GDPR da UE não se aplica no Reino Unido, tendo sido substituído pelo GDPR do Reino Unido (GDPR UK). O GDPR UK entrou oficialmente em vigor em 01 de janeiro de 2021, sendo amplamente no GDPR da UE, com algumas mudanças pontuais para torná-lo mais eficaz no contexto britânico.<sup>55</sup>

A Lei de Proteção de Dados (*Data Protection Act*, DPA) de 2018, que estabeleceu a estrutura de proteção de dados no Reino Unido, também foi alterada em 01 de janeiro de 2021 para refletir o status do Reino Unido fora da UE. A DPA foi adaptada para ser lida em conjunto com o novo GDPR do Reino Unido. Ela se situa ao lado e complementa o GDPR do Reino Unido - por exemplo, estabelecendo exceções. Também estabelece regras separadas de proteção de dados para as autoridades de aplicação da lei (*law enforcement*), estende a proteção de dados a algumas outras áreas, como segurança nacional e defesa, e estabelece as funções e poderes do *Information Commissioner's Office* (ICO), autoridade de proteção de dados do Reino Unido.

A proteção de dados de pacientes é regrada por legislação ordinária que trata do sigilo médico e as informações confidenciais do paciente, além da legislação de proteção de dados.

As informações do paciente são dados pessoais nos termos da legislação de proteção de dados se forem identificáveis, ou tiverem o potencial de serem identificados, com base nas informações mantidas pela organização que detém os dados. Portanto, as informações sobre o paciente podem ser desidentificadas para um pesquisador, mas ainda assim classificadas como dados pessoais no que diz respeito à organização que detém os dados.

Para processar dados pessoais, a GDPR e a Lei de Proteção de Dados de 2018 exigem que o operador tenha uma base legal. O NHS recomenda que as organizações de pesquisa que são autoridades públicas utilizem como base o interesse público e que os parceiros de pesquisa comercial utilizem o legítimo interesse como base legal. O consentimento explícito nos termos do GDPR não é necessário para pesquisas de saúde.<sup>56</sup> Já a coleta e tratamento de dados no atendimento primário, com médicos hospitalares e clínicas decorre de cumprimento de obrigação legal.

Sendo um sistema com centralização no governo, o NHS usa a digitalização de informações e cruza informações de maneira intensa.<sup>57</sup> Há um esforço ativo do NHS para intensificar o uso de tecnologia e cruzamento de dados, visto que o uso interoperável destas informações é benéfico para o planejamento das ações de saúde e para a atenção e cuidado aos pacientes. Não apenas o tratamento de doenças é diretamente melhorado,

---

55 Cf.: <https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-dpa-2018/about-the-dpa-2018/>

56 Cf.: <https://www.hra.nhs.uk/covid-19-research/guidance-using-patient-data/>.

57 Cf.: <https://digital.nhs.uk/about-nhs-digital>.

mas o Health Data Research UK58 utiliza-se de dados estatísticos para gerar melhoras na eficiência do sistema de saúde. Assim, a NHS não deixa de cruzar dados de pacientes, mas utilizam-se de “de-identification” para os casos em que seu uso de dados é de para planejamento e pesquisa.<sup>59</sup>

Um membro da equipe de atendimento de um paciente ou usuário de serviço pode anonimizar informações confidenciais do paciente de modo a não violar o dever de confidencialidade. A equipe de atendimento inclui profissionais de saúde e de assistência social registrados e outros funcionários que prestam ou apoiam diretamente o atendimento aos pacientes. As informações anônimas podem então ser usadas em pesquisas de saúde e cuidados.<sup>60</sup>

O NHS reconhece que não pode analisar todas as informações de saúde dos pacientes por si só, de modo que compartilham informações com pesquisadores, analistas e organizações que “são especialistas em dar sentido a informações complexas”. O órgão afirma compartilhar “apenas o que é necessário para cada pesquisa e, sempre que possível, a informação é removida” para que o usuário não possa ser identificado.<sup>61</sup>

A partir de 25 de maio de 2018, os cidadãos podem optar por impedir que suas informações confidenciais de saúde sejam usadas para outros fins que não sejam seus próprios cuidados e tratamento. Esta escolha é conhecida como *opt-out* nacional de dados (*national data opt-out*). Se o usuário do sistema de saúde optar por não participar seus dados, o NHS Digital aplicará sua exclusão a partir de 25 de maio de 2018. Todas as outras organizações de saúde e assistência social foram obrigadas a aplicar sua exclusão até 30 de setembro de 2021.<sup>62</sup>

Com o *General Practice Data for Planning and Research* (GPDPR), os profissionais de saúde primária deverão obrigatoriamente fazer o *upload* automático dos dados dos pacientes para o sistema de TI do governo britânico, compartilhando-os com o NHS digital, a menos que a pessoa tenha *optado por sair* (*opt-out*) do esquema de compartilhamento de dados para pesquisa e planejamento. Os dados compartilhados incluem dados sobre sexo, etnia e orientação sexual; códigos clínicos e dados sobre diagnósticos, sintomas, observações, resultados de testes, medicamentos, alergias, imunizações, encaminhamentos, consultas e retorno, incluindo informações sobre a saúde física, mental e sexual dos pacientes, dados da equipe que realizou o atendimento, além de demais dados estabelecidos nas diretrizes do Aviso de Fornecimento de Dados enviado para clínicas de atenção primária<sup>63</sup>.

Não serão compartilhados: nome e endereço (exceto “CEP” em forma codificada única); notas escritas (texto livre), tais como os detalhes das conversas com médicos e enfermeiros; imagens, cartas e documentos; dados codificados que não são necessários

---

58 Cf.: <https://www.hdr.uk/about-us/what-we-do/health-data-research-explained/>.

59 Cf.: [https://digital.nhs.uk/services/master-person-service\\_](https://digital.nhs.uk/services/master-person-service_)

60 Cf.: <https://www.hra.nhs.uk/covid-19-research/guidance-using-patient-data/>

61 Cf.: <https://www.nhs.uk/using-the-nhs/about-the-nhs/sharing-your-health-records/>

62 Cf.: <https://www.nhs.uk/your-nhs-data-matters/>

63 Cf.: <https://westheathprimarycarecentre.nhs.uk/2021/06/07/general-practice-data-for-planning-and-research-nhs-data-opt-out/>



devido a sua idade - por exemplo, medicação, encaminhamento e dados de consulta com mais de 10 anos de idade; dados codificados cujo compartilhamento não é autorizado – por exemplo, certos códigos sobre o tratamento de fertilização e certas informações sobre a mudança de sexo.

O programa sofreu duras críticas, sobretudo pela inclusão no sistema de compartilhamento *by default*, além da falta de transparência e publicidade quanto a sua aplicação. Uma pesquisa realizada próximo à data original de *opt-out* apontou que apenas 55% dos entrevistados já haviam ouvido falar do compartilhamento de seus dados, e que 71% dos entrevistados acreditavam que o NHS não tornou o esquema público o suficiente<sup>64</sup>. Com isso, a data de início de coleta compulsória dos dados foi adiada, com três objetivos específicos: desenvolver um processamento centralizado e automático de opt-outs e opt-ins, para reduzir a carga sobre os GPs; tornar os dados disponíveis somente através de um sistema online seguro, conhecido como Ambiente de Pesquisa Confiável (*Trusted Research Environment, TRE*); permitir mais tempo para uma campanha de conscientização pública para garantir que o público esteja ciente de suas escolhas de dados<sup>65</sup>.

### 2.7.3 Saúde digital no Reino Unido e interoperabilidade

Em 7 de janeiro, de 2019 foi publicado o plano de longo prazo do NHS (anteriormente conhecido como o plano de 10 anos) que estabelece as principais ambições para o serviço nos próximos 10 anos.<sup>66</sup>

A tecnologia digital está por trás de algumas das metas mais ambiciosas do plano, voltadas para o paciente. O aplicativo do NHS atuará como uma porta de entrada para que as pessoas tenham acesso a serviços e informações; até 2020/21, as pessoas poderão usá-lo para acessar seu plano de atendimento e comunicações dos profissionais de saúde. A partir de 2024, os pacientes terão um novo “direito” de acesso aos serviços digitais de atendimento primário (por exemplo, consultas on-line), seja através de sua prática existente ou através de novos serviços emergentes. Ao final do período de 10 anos abarcado pelo plano, a perspectiva é que as pessoas sejam cada vez mais atendidas e assistidas em casa usando monitoramento remoto (através de dispositivos “wearable”) e ferramentas digitais. Espera-se que a tecnologia digital também facilite a transformação de serviços, incluindo o redesenho de serviços ambulatoriais e reorganizações de serviços de patologia e diagnóstico por imagem.

Para oferecer o atendimento digital, como previsto, o plano reitera a ambição previamente declarada de que todos os provedores de atendimento secundário sejam “totalmente digitalizados” até 2024 (um prazo que se afastou da meta original de 2020). Isso implicará a criação de registros eletrônicos e uma série de outras capacidades digitais por

---

64 Cf.: <https://www.which.co.uk/news/2021/07/nhs-patient-data-sharing-what-you-need-to-know-about-gdpr/>

65 Cf.: <https://www.healthcareitnews.com/news/emea/uk-government-halts-gp-data-sharing-scheme-after-mistakes-were-made>

66 Cf.: <https://www.gov.uk/government/news/nhs-long-term-plan-launched#:~:text=The%2010%2Dyear%20plan%20includes,services%20for%20adults%20and%20children.&text=The%20NHS%20Long%20Term%20Plan,patient%20care%20and%20health%20outcomes.>

parte das organizações do NHS. O programa *Global Digital Exemplars* admitirá novas organizações e criará modelos para adoção de tecnologia e um registro compartilhado através de Exemplos de Registros Locais de Saúde e Cuidados com a Saúde (*Local Health and Care Record Exemplars*).

Para promover a interoperabilidade, há agora um compromisso de introduzir controles durante 2019 para assegurar que os fornecedores de tecnologia do NHS cumpram com as normas acordadas.<sup>67</sup>

Nessa implantação da digitalização e interoperabilidade, o NHS Digital (*Health and Social Care Information Centre*) tem o papel de fornecedor nacional de informações, dados e sistemas de TI para comissários, analistas e clínicos em saúde e assistência social na Inglaterra, particularmente aqueles envolvidos com o Serviço Nacional de Saúde da Inglaterra. A organização é um órgão público executivo não departamental do Departamento de Saúde e Assistência Social.

O NHS Digital fornece serviços digitais para o NHS e assistência social, incluindo a gestão de grandes programas de informática de saúde. O NHS Digital presta serviços digitais no âmbito nacional através de equipes internas e da contratação de fornecedores privados. Estes serviços incluem o gerenciamento de dados dos pacientes, incluindo o *Spine*.

O *Spine* oferece suporte à infraestrutura de TI para a saúde e a assistência social na Inglaterra, unindo mais de 23.000 sistemas de TI para a saúde em 20.500 organizações. O sistema *Spine* permite que as informações sejam compartilhadas com segurança através de serviços nacionais, tais como que permite o compartilhamento seguro de informações entre diferentes partes do NHS, e forma a base do Serviço de Prescrição Eletrônica (*Electronic Prescription Service*)<sup>68</sup>, do Registro Sumário de Cuidados (*Summary Care Record*)<sup>69</sup>, do Serviço de Encaminhamento Eletrônico (*Electronic Referral Service*)<sup>70</sup> e do Sistema de Compartilhamento de Informações e Proteção à Criança (*Child Protection - Information Sharing system*)<sup>71</sup>.

Segundo o NHS, para proporcionar uma jornada de cuidados contínua, é importante que as tecnologias relevantes no sistema de saúde e assistência social sejam interoperáveis, em termos de hardware, software e os dados contidos no mesmo. O NHS Digital hospeda um conjunto de ferramentas de interoperabilidade para apoiar as aplicações informáticas.

---

67 Cf.: <https://www.kingsfund.org.uk/publications/nhs-long-term-plan-explained#introduction>

68 O Serviço de Prescrição Eletrônica envia prescrições digitais de cirurgias de médicos de clínica geral e outros profissionais do NHS para farmácias, sem necessidade de prescrição médica impressa

69 O Registro Sumário do Paciente permite ao pessoal autorizado do NHS (como o staff do hospital ou da ambulância) ver um resumo de informações importantes sobre um paciente, para ajudar a dar o melhor atendimento

70 Administra a reserva de consultas pela primeira vez com hospitais e especialistas.

71 Ajuda a garantir que qualquer preocupação com a proteção de crianças seja conhecida pelo NHS quando elas são tratadas.

Também se considera importante que os dados sejam registrados de uma forma padronizada específica, pois isso permite que informações úteis sejam coletadas de múltiplas fontes, para somar cuidados, o que pretende ser alcançado seguindo padrões abertos. Dentro do sistema inglês de saúde e assistência social, os padrões de informação impõem as especificações usadas para coletar e extrair dados dos sistemas de tecnologia da informação<sup>72</sup>.

É necessário demonstrar que uma tecnologia de saúde - e seus sistemas *back-end* - compartilham dados com outros sistemas clínicos dentro das regras apropriadas relativas à captura, apresentação, compartilhamento e armazenamento de dados. Em outras palavras, se uma tecnologia precisa se comunicar com sistemas clínicos para compartilhar dados, ela deve estar em conformidade com as normas clínicas, profissionais e técnicas relevantes. Existem normas que criam uma 'linguagem' comum no registro de dados de saúde e as tecnologias digitais de saúde devem utilizá-las.<sup>73</sup>

Com novos modelos de atendimento surgindo e evoluindo, o NHS tem advogado pela clara necessidade de um compartilhamento de informações mais eficaz entre ambientes de atendimento, assim como entre profissionais e cidadãos, para otimizar os resultados dos pacientes e a qualidade do atendimento. Isso depende da capacidade dos sistemas de TI em toda a área da saúde de serem interoperáveis entre si, o que seria fundamental para a concretização da visão futura dos cuidados na Inglaterra.<sup>74</sup>

O NHS afirma serem necessárias formas mais integradas de trabalho na área da saúde e do atendimento para permitir que os profissionais de saúde e os cidadãos gerenciem melhor o atendimento, em um esforço conjunto com organizações que oferecem novos modelos de cuidados e iniciativas sendo impulsionadas por sistemas integrados de cuidados. O movimento em direção à interoperabilidade de todo o NHS concentra-se nas seguintes áreas<sup>75</sup>:

- i) Trabalhar com serviços para identificar suas necessidades comerciais estratégicas em relação à interoperabilidade para informar o desenvolvimento das soluções necessárias;
- ii) Desenvolvimento de estudos de uso prioritário para interoperabilidade a fim de fornecer justificção comercial para investimento local e desenvolvimento de sistemas e produtos de apoio a nível nacional;
- iii) Oferecer apoio às organizações locais com ferramentas e orientações que lhes permitam desenvolver soluções eficazes para os problemas de interoperabilidade;
- iv) Desenvolver padrões para apoiar a mudança do "papel" para as "transferências eletrônicas de cuidados";

72 Cf.: <https://digital.nhs.uk/data-and-information/information-standards>

73 Cf.: <https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology#section-10>

74 Cf.: <https://www.gov.uk/government/publications/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care#cs12-main>

75 Cf.: <https://www.england.nhs.uk/digitaltechnology/connecteddigitalsystems/interoperability/>

- v) Desenvolvimento de padrões para apoiar a mudança para sistemas que permitam o acesso às informações do paciente através de interfaces abertas (CareConnect APIs);
- vi) Comissionamento do NHS Digital na entrega de normas de interoperabilidade;
- vii) Trabalhar com a plataforma INTEROPen na adoção da interoperabilidade.

O modelo de saúde digital inclui também a previsão de portabilidade de dados de prontuários médicos e registros de saúde em um ambiente de competição entre os médicos, conforme indicado acima. A plataforma GP2GP (“General practitioners to General practitioner”, que poderia ser traduzido livremente como “de clínico geral para clínico geral”) permite que os registros eletrônicos de saúde dos pacientes sejam transferidos diretamente, com segurança e rapidez entre seus antigos e novos médicos, quando eles mudam de médico generalista. A iniciativa visa a melhorar o atendimento ao paciente ao disponibilizar prontuários completos e detalhados aos consultórios, para as primeiras e posteriores consultas de um novo paciente.

O *General Medical Services GP Contract* requer que os clínicos gerais utilizem o GP2GP para a transferência de registros de saúde eletrônicos, apoiando o objetivo da Secretaria de Saúde de que os pacientes tenham seus registros eletrônicos de saúde acessíveis em todas as etapas do seu atendimento de saúde.

#### 2.7.4 Conclusões parciais sobre o sistema inglês

A partir da análise delineada acima sobre o sistema inglês de saúde, prontuários eletrônicos e interoperabilidade pode-se depurar o seguinte:

- i) O sistema de saúde inglês é centralizado em nível nacional, com predomínio quase que absoluto de financiamento e prestação de serviço público de saúde;
- ii) O governo britânico tem investido massivamente em programa público de digitalização dos serviços de saúde e implantação do *e-health*, com a adoção de diversas padronizações e ferramentas para a interoperabilidade entre os serviços, inclusive com a gestão centralizada de informática e sistemas de TI empregados no plano nacional;
- iii) Nesse modelo centralizado também há a concentração dos dados médicos do paciente cujo upload é feito pelos médicos e profissionais de saúde, mas o acesso aos mesmos deve se dar no contexto de tratamento e atendimento, preservando-se sua privacidade;
- iv) Os dados do sistema nacional de saúde, que inclui os dados dos pacientes, podem receber tratamento para usos secundários, em particular, para pesquisa e definição de políticas públicas, porém para tais usos os dados passam por desidentificação e o paciente pode optar por recusar que os dados sejam utilizados para outros fins que não o atendimento imediato a saúde (*opt out*);
- v) O sistema de *opt out* para uso secundário (pesquisa e políticas públicas) sofre várias críticas por entidades médicas e de proteção de dados, uma vez que

por padrão, e sem o consentimento expresso do paciente, os dados são processados pelo governo;

- vi) Considerando que a camada competitiva no modelo de saúde inglês está na atuação dos médicos (que concorrem pelos pacientes) adota-se a portabilidade dos dados de saúde entre médicos, ou seja, quando o paciente troca de médico, tem o direito de portar todos os dados e anotações sobre sua saúde;
- vii) Como praticamente é inexistente a saúde complementar privada na Inglaterra, não há questão acerca do compartilhamento de dados com seguradoras privadas.

## 2.8 Estados Unidos da América

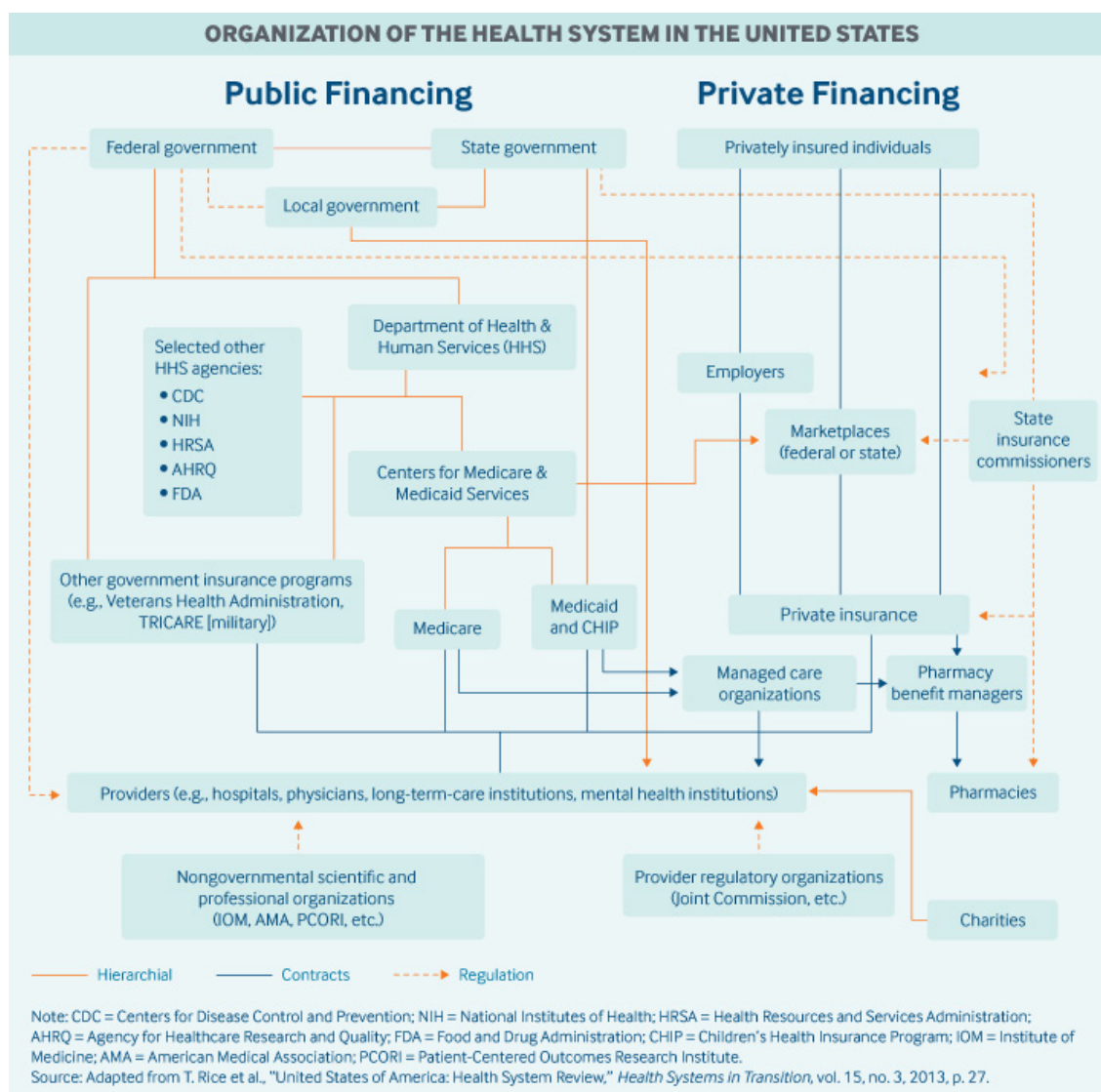
### 2.8.1 O sistema de saúde dos EUA

O sistema de saúde dos EUA é um sistema misto, que conta com seguradoras e prestadores de serviços de saúde públicos e privados, com e sem fins lucrativos. O governo federal fornece fundos para o programa nacional *Medicare*, destinado a adultos com 65 anos ou mais e para pessoas com determinadas deficiências, bem como para vários programas para veteranos de guerra e pessoas de baixa renda, incluindo o *Medicaid* e o Programa de Seguro de Saúde para Crianças (*Children's Health Insurance Program*), ao passo que os estados da federação administram e pagam por aspectos da cobertura local e da rede de segurança. O seguro privado, a forma dominante de cobertura, é fornecido principalmente pelos empregadores. A taxa de não segurados caiu de 16% para 8,5% da população em 2010, o ano em que a lei *Affordable Care Act* foi promulgada. As seguradoras públicas e privadas estabelecem seus próprios pacotes de benefícios e estruturas de compartilhamento de custos, dentro dos regulamentos federais e estaduais<sup>76</sup>.

---

76 **United States.** Disponível em: <<https://www.commonwealthfund.org/international-health-policy-center/countries/united-states>>. Acesso em: 11 mar. 2022.

A organização do sistema de saúde dos EUA se encontra esquematizado no infográfico abaixo<sup>77</sup>:



## 2.8.2 O uso de dados pessoais no setor de saúde dos EUA

### 2.8.2.1 O HIPAA e o HITECH

Os EUA abordam a privacidade e proteção de dados de forma setorial e em diferentes esferas. Para dados relacionados à saúde, a legislação principal é o *Health Insurance and Portability and Accountability Act* (HIPAA), pelo qual diferentes dados de saúde são protegidos de forma distinta. A sobreposição de tipos de proteção de dados de saúde e de diferentes sistemas e equipamentos que geram dados conectados à saúde de indivíduos fazem com que "a privacidade de dados de saúde seja incrivelmente complexa e desafiadora".<sup>78</sup>

77 **United States.** Disponível em: <<https://www.commonwealthfund.org/international-health-policy-center/countries/united-states>>. Acesso em: 11 mar. 2022.

78 KOONTZ, L. D. (ED.). **Information privacy in the evolving healthcare environment.** Chicago,

O HIPAA foi aprovado em 1996 com o objetivo de proteger as informações de saúde de indivíduos, mas também possibilitar o compartilhamento de informação para garantir um atendimento médico de qualidade. O HIPAA foi derivado dos *Fair Information Practice Principles* (FIPPs) de Westin<sup>79</sup>. Seus termos especificam quem está coberto pela proteção, qual informação é protegida e como a informação de saúde protegida pode ser usada e distribuída. A lei busca antecipar os compartilhamentos necessários para políticas públicas e estabelecer limites rígidos para outras formas de compartilhamento. Ao contrário de outras regulações baseadas nos FIPPs, o HIPAA elevou a escolha individual e consentimento a um princípio e deu maior ênfase à prestação de contas e responsabilização, inclusive com a notificação de incidentes de dados.

O HIPAA regula “atividades cobertas” e seus “business associates” para proteger apenas “informação de saúde” identificáveis. Assim, é aplicável a provedores de saúde, planos de saúde, empresas seguradoras de saúde que processam informações de saúde. Determina que apenas a quantidade mínima de informações seja coletada e distribuída para cada atividade, e que organizações devem determinar qual é esse mínimo. Ainda, adotou uma abordagem de *notice-and-consent* em que pacientes autorizam a distribuição dos seus dados de saúde, introduzindo a noção de *consentimento individual*, e incluindo considerações especiais para dados de menores.

As regulações de privacidade do HIPAA são supervisionadas pelo *Office for Civil Rights* (OCR) no Departamento de Saúde e Serviços Humanos (HSS). Considerando que o HIPAA foi redigido em uma época em que a maior parte dos prontuários médicos eram mantidos em papel, a emergência das tecnologias de informação e bases de dados computacionais demandou adaptação. O fato de que o HSS foi autorizado a regulamentar aspectos de privacidade possibilitou que o HIPAA respondesse às novas tecnologias, mas algumas mudanças tecnológicas ainda não são adequadamente contempladas. Depois de uma grande atualização em 2003 e da entrada em vigor do *Final Omnibus Rule* em 2013, o OCR passou a preferir emitir *guidelines* (em vez de regulamentações).

O HIPAA também permite o uso secundário de dados para propósitos como pesquisa, saúde pública, *law enforcement*, procedimentos judiciais, e outras “atividades de interesse e benefício público” (nos termos da “Regra de Privacidade” da Lei), sem autorização individual. Mesmo em casos de casos sensíveis, estes podem ser requisitados para fins de saúde pública, *law enforcement*, e o monitoramento de sinais vitais, entre outros. A nível estatal, a lei pode requerer que indivíduos compartilhem dados pessoais para fins escolares ou para a obtenção de licenças (como casamento, compra de armas e direção).

Caso esses dados sejam utilizados para pesquisa, é necessária a autorização dos pacientes, e pesquisadores devem desidentificar os dados. O HIPAA governa o processo de desidentificação de dados para proteger a privacidade, especificando dois métodos: determinação individual por um expert qualificado e *safe harbor*. A remoção das informações de saúde pessoais (ou protegidas) – conhecidas como PHI (*Personal Health Information*) – é considerada suficiente para proteger a privacidade. Sem PHI, o HIPAA não se aplica mais aos dados em questão.

Para adaptar o HIPPA a nova realidade da tecnologia digital e ao uso de prontuários eletrônicos, foi promulgada, em 2009, a lei *Health Information Technology for Economic and Clinical Health* (HITECH). Tendo em vista o agravamento dos riscos relativos à privacidade, o HITECH fortalece o HIPPA e estimula a digitalização. Em primeiro lugar, a lei promove a digitalização criando subsídios para que clínicas e estabelecimentos de saúde que atendem pacientes do Medicare adotassem o prontuário eletrônico, com o objetivo de fazer com que todos aqueles envolvidos no atendimento e cuidado do paciente pudessem ter acesso aos dados de seu histórico de saúde. Em segundo lugar, trouxe incentivos para facilitar o compartilhamento comercial de dados para a pesquisa pública. Em terceiro, criou um centro de trocas de informação estatal (Health Information Exchanges-HIE), para ser ligado a um sistema nacional de redes de informação (National Health Information Network- NHIN) para fazer com que os dados médicos de cada pessoa fossem acessíveis no ponto de cuidado, quando necessário para um procedimento médico, assim como para pesquisa e biossegurança.

Importante destacar que essa rede de informações traz uma *interoperabilidade de dados*, na qual se viabiliza o acesso pelos profissionais de saúde envolvidos em um procedimento de tratamento, de modo que não se trata de compartilhamento de prontuários médicos com seguradoras, cujos dados a serem compartilhados, dependem do consentimento do paciente, que é a regra primordial do HIPPA.

### **2.8.2.2 Covid-19 e alterações no HIPPA**

Durante a pandemia do coronavírus, o aumento da vigilância e a divulgação de dados de saúde diminuíram a capacidade dos pacientes de manter o sigilo sobre seu estado de saúde. Em resposta à declaração de emergência nacional relativa à COVID-19, o Departamento de Saúde e Serviços Humanos (HHS) anulou e modificou partes do HIPPA referente à privacidade dos pacientes. As novas modificações no HIPAA passaram a permitir que as informações dos pacientes fossem compartilhadas, independentemente de consentimento, para ajudar em emergências de saúde pública em todo o país e para ajudar os pacientes a receber os cuidados de que necessitam.

Essas modificações no HIPAA foram feitas menos de duas semanas depois que a Administração divulgou duas regras federais amplamente aguardadas sobre compartilhamento de dados de saúde destinadas a dar aos pacientes um acesso eletrônico mais fácil aos seus registros médicos e alimentar um compartilhamento mais livre de dados de saúde. Após um ano de intenso lobby sobre as regras propostas, as regras finais foram emitidas por duas agências diferentes dentro do Departamento de Saúde e Serviços Humanos (*Department of Health and Human Services, HHS*), o Escritório do Coordenador Nacional de Tecnologia da Informação em Saúde (*Office of the National Coordinator for Health Information Technology, ONC*) e os Centros de Serviços de Medicare e Medicaid (*Centers for Medicare and Medicaid Services, CMS*).

### 2.8.3 Saúde digital e interoperabilidade nos EUA

Com as novas regras referentes ao uso de dados pessoais de saúde, as pessoas poderão, pela primeira vez, usar aplicativos de sua escolha para acessar dados como resultados



de exames de sangue, medições de pressão arterial e uma infinidade de outros resultados de dados pessoais de saúde diretamente de seus provedores de saúde. De acordo com o HHS, o novo sistema foi concebido para “*tornar tão fácil para as pessoas gerenciar seus cuidados de saúde em smartphones quanto para elas usar aplicativos para gerenciar suas finanças*”<sup>80</sup>. As novas regras de acesso dos pacientes fazem parte de um esforço geral para facilitar a movimentação de dados dos pacientes de um ambiente para outro.

A principal regra da ONC exige que os fornecedores de registros eletrônicos de saúde adotem softwares, conhecidos como interfaces de programação de aplicativos (APIs), para permitir que os fornecedores enviem dados de registros médicos diretamente para aplicativos autorizados pelo paciente. Os médicos e centros médicos são obrigados a enviar um conjunto central de dados médicos para aplicações de terceiros após um paciente ter autorizado o intercâmbio de dados de saúde. Os dados podem incluir informações pessoais do paciente, tais como resultados de exames laboratoriais e sinais vitais, além de notas clínicas sobre cirurgias de um paciente, estadias hospitalares, testes de imagem e resultados de patologia. O uso de software API permitirá que os pacientes utilizem aplicativos para obter suas reclamações de seguro e informações sobre benefícios.

Os provedores de saúde e fornecedores de registros de saúde eletrônicos tiveram dois anos (as regras entram em vigor em 2022) para cumprir com os requisitos referentes à API. Os médicos e fornecedores de registros de saúde eletrônicos que dificultarem tal compartilhamento de dados – uma prática chamada bloqueio de informações (*information blocking*) – estão sujeitos a investigação federal e multas.

### **2.8.3.1 21st Century Cures Act (Cures Act)**

A 21st Century Cures Act (Lei das Curas do Século 21), assinada em 13 de dezembro de 2016, foi concebida para ajudar a acelerar o desenvolvimento de produtos médicos e trazer novas inovações e avanços aos pacientes que deles necessitam de forma mais rápida e eficiente. A lei se baseia no trabalho contínuo da *Federal Drugs Agency* (FDA) – órgão com atuação semelhante à da Anvisa no Brasil – para incorporar as perspectivas dos pacientes no desenvolvimento de medicamentos, produtos biológicos e dispositivos no processo decisório da FDA.

O Escritório da ONC, a agência federal que supervisiona a tecnologia da informação em saúde, anunciou, em 5 de abril de 2021, uma lista há muito esperada sobre quais dados eletrônicos de saúde devem ser disponibilizados aos pacientes e aos provedores de serviços de saúde. Segundo o órgão, isso representa um passo significativo para melhorar a qualidade do atendimento quando os pacientes consultam vários médicos e garantir que os indivíduos possam visualizar seus registros de maneira facilitada. As mudanças pretendem alavancar o compartilhamento e o acesso aos dados<sup>81</sup>.

---

80 **Individuals’ Access and Use of Patient Portals and Smartphone Health Apps, 2020 | HealthIT.gov.** Disponível em: <<https://www.healthit.gov/data/data-briefs/individuals-access-and-use-patient-portals-and-smartphone-health-apps-2020>>. Acesso em: 11 mar. 2022.

81 **A New Day for Interoperability – The Information Blocking Regulations Start Now.** Disponível em: <<https://www.healthit.gov/buzz-blog/information-blocking/a-new-day-for-interoperability-the-informa->

Dentro do contexto da 21st Century Cures Act, o Congresso usou o termo “bloqueio de informações” para se referir à falha consistente em compartilhar dados efetivamente com médicos e prestadores de serviços de saúde que estão autorizados a visualizá-los. As novas regras da ONC, que foram introduzidas em maio de 2020, enfrentam esse problema ao exigir que as informações armazenadas nos registros eletrônicos de saúde (*electronic health records*, EHR) sejam compartilhadas com qualquer pessoa que tenha o direito legal de acessá-las, como os próprios pacientes ou diferentes prestadores de serviços de saúde que eles visitem. Qualquer prestador de serviços de saúde ou fornecedor de TI de saúde que viole tais regras poderia enfrentar penalidades financeiras.

De acordo com o anúncio da ONC, os provedores de serviços de saúde, desenvolvedores de sistemas de TI de saúde certificados pelo governo federal devem ser capazes de compartilhar todos os dados da primeira versão do que é conhecido como o conjunto de dados centrais para interoperabilidade dos Estados Unidos (*United States Core Data for Interoperability*, USCDI)<sup>82</sup>. O USCDI se refere, portanto, ao conjunto de dados nacional que os EHRs devem ser capazes de acessar e compartilhar. Além das informações demográficas (como raça, idade e sexo), ele inclui informações clínicas vitais no EHR de um indivíduo. Por exemplo, o EHR deve ser capaz de compartilhar as alergias, imunizações e resultados de testes laboratoriais dos pacientes, bem como os medicamentos recebidos e quaisquer notas clínicas de médicos que possam lançar luz sobre seus cuidados.

Para a ONC, essas informações podem auxiliar os diferentes profissionais da saúde que atendem o mesmo paciente, como quando um médico de cuidados primários encaminha um indivíduo a um especialista, pois compartilhar esses dados eletronicamente tornaria mais fácil para o novo profissional compreender o histórico médico de um paciente e determinar o curso apropriado do tratamento. Além disso, a pandemia de COVID-19 destacou como as lacunas no compartilhamento eletrônico de dados podem forçar as autoridades de saúde pública a compartilhar resultados de testes ou registros de vacinas usando métodos antiquados, tais como o fax. O uso de tais tecnologias pode acrescentar encargos de entrada de dados e tornar mais difícil para as agências de saúde pública responder a crises de saúde de forma oportuna, de modo que um melhor intercâmbio eletrônico de dados poderia ajudá-los a enfrentar futuros surtos de doenças<sup>83</sup>.

Esse incentivo para tornar os dados de saúde mais uniformes e disponíveis aos provedores de serviços de saúde e pacientes também se enquadra nos desejos da maioria dos americanos. Uma pesquisa encomendada pela *The Pew Charitable Trusts* constatou que a maioria dos entrevistados queria ter acesso aos dados em seus EHRs, tais como registros de imunização, resultados de testes de laboratório e notas clínicas. Eles também apoiaram amplamente que os vários profissionais que visitam pudessem compartilhar esses dados uns com os outros.<sup>84</sup>

tion-blocking-regulations-start-now>. Acesso em: 11 mar. 2022.

82 **United States Core Data for Interoperability (USCDI)**. Disponível em: <<https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi>>. Acesso em: 11 mar. 2022.

83 **Biden Administration Should Improve Data Exchange Practices to Promote Public Health**. Disponível em: <<https://pew.org/37WJ5bi>>. Acesso em: 11 mar. 2022.

84 **Americans Want Federal Government to Make Sharing Electronic Health Data Easier**. Disponível em: <<https://pew.org/3hqjFEV>>. Acesso em: 11 mar. 2022.

O anúncio da ONC é um primeiro passo em direção ao compartilhamento e a interoperabilidade da base de dados de saúde nos EUA. Em outubro de 2022, a agência vai exigir que os profissionais de saúde, hospitais e outros grupos afetados, como os HIEs, compartilhem informações de saúde eletrônicas. Isto incluirá dados além dos que estão no USCDI, tais como quando uma doença foi diagnosticada ou tratada, assim como informações sobre imagens de diagnóstico, inclusive o momento em que foram solicitadas e o que elas mostraram (a agência está incentivando fornecedores e profissionais a compartilhar dados adicionais antes disso, mas não será, até lá, uma exigência).

O Escritório da ONC anunciou que a Estrutura de Intercâmbio Confiável e o Acordo Comum (*Trusted Exchange Framework and Common Agreement, TEFCA*) serão concluídos até 2022<sup>85</sup>. O TEFCA é parte da *21st Century Cures Act* e tem como objetivo estabelecer diretrizes para padrões de interoperabilidade para redes de informação sanitária qualificada (*qualified health information networks, QHINs*) em todos os Estados Unidos. O objetivo é criar padrões de compartilhamento de dados e uma estrutura para QHINs a serem seguidos, que deverão aumentar a segurança e agilizar o compartilhamento de dados entre EHRs para evitar o bloqueio de informações, intencional ou não. O Coordenador Nacional da ONC, Micky Tripathi, enfatizou que o compartilhamento de informações é fundamental para aumentar a interoperabilidade entre os provedores e a implementação do TEFCA pode ser uma parte fundamental desse objetivo<sup>86</sup>.

### 2.8.3.2 United States Core Data for Interoperability (USCDI)

O USCDI é o conjunto padronizado de classes de dados de saúde e elementos de dados constituintes para o intercâmbio de informações de saúde interoperáveis em todo o país. Em 15 de abril de 2021, o Comitê Consultivo de Tecnologia da Informação em Saúde, estabelecido pelo Congresso no *21st Century Cures Act*, aprovou unanimemente as recomendações de sua Força Tarefa de Dados Básicos para Interoperabilidade dos EUA (USCDI) para expandir significativamente os elementos de dados incluídos nos dados básicos para interoperabilidade a nível nacional.

Em outras palavras, o USCDI corresponde ao conjunto de dados estruturados de saúde essenciais para a interoperabilidade nacional, troca eletrônica de informações de saúde e usabilidade, sem que seja necessário o emprego de esforço especial para esses fins. O conjunto de dados é utilizado para encaminhamento e transferências de cuidados, para a troca de dados através de interfaces de programação de aplicações (APIs) padronizadas, e para acesso do paciente para visualizar, baixar e transmitir dados de saúde a qualquer terceiro, incluindo aplicações (aplicativos) de saúde de terceiros.

A ONC divulgou o rascunho original do USCDI em 2018. O documento listou 50 elementos de dados para potencial adição ao já existente *Common Clinical Data Set* (conjunto de dados clínicos comuns, em tradução literal). A ONC afirmou que todos os dados

---

85 ONC says TEFCA will be live in 2022. Disponível em: <<https://www.healthcareitnews.com/news/onc-says-tefca-will-be-live-2022>>. Acesso em: 11 mar. 2022.

86 **Key Takeaways from Micky Tripathi's SHIEC 2021 Keynote.** Disponível em: <<https://ainq.com/key-takeaways-from-micky-tripathi-shiec-2021-session/>>. Acesso em: 11 mar. 2022.

listados são “críticos para alcançar a interoperabilidade nacional”, que as especificações técnicas já estavam disponíveis para 46 dos 50 elementos e classes de dados. Em maio de 2020, a ONC fez uma “modesta expansão” do Conjunto Comum de Dados Clínicos (embora houvesse algumas adições importantes, tais como notas clínicas e de procedência)<sup>87</sup>.

### 2.8.3.3 Cures Act Final Rule

A *Final Rule* do 21<sup>st</sup> Century Cures Act tem como objetivo implementar os requisitos de interoperabilidade estabelecidos no *Cures Act*, a partir da perspectiva de que os pacientes “precisam de mais poder em seus cuidados com a saúde, e o acesso à informação é fundamental para que isso aconteça”<sup>88</sup>.

Essa “regra final” implementa certas disposições da 21st Century Cures Act, incluindo Condições e Manutenção dos requisitos de Certificação para desenvolvedores de tecnologia da informação em saúde sob o Programa de Certificação de TI em saúde do ONC, a certificação voluntária de TI em saúde para uso por provedores de cuidados de saúde pediátricos, e atividades razoáveis e necessárias que não constituem bloqueio de informação. A implementação destas disposições fará avançar a interoperabilidade e apoiará o acesso, o intercâmbio e o uso de informações eletrônicas de saúde. A regra também conclui certas modificações nos critérios e no Programa de certificação de TI em saúde de 2015, de forma adicional a incentivar a interoperabilidade, melhorar a certificação de TI em saúde e reduzir a carga e os custos referentes a esses processos. A regra entrou em vigência em 30 de junho de 2021.<sup>89</sup>

De maneira geral, os objetivos da “regra final” convergem no sentido de permitir que o sistema de saúde promova maior transparência sobre o custo e os benefícios/resultados dos serviços de cuidados em saúde dos pacientes; promover a competição entre fornecedores e fornecer opções competitivas para os pacientes quando da escolha dos serviços; o desenvolvimento de aplicações para smartphones que permitam ao paciente um melhor controle de seus dados de saúde; a promoção de uma economia baseada em tecnologias da informação que permitam aos pacientes, médicos, hospitais, empregadores e seguradoras a buscar inovação e maior liberdade no que se refere aos cuidados em saúde.

### 2.8.4 Compartilhamento com seguradoras e preocupações em relação a empresas de TI

Na linha dos regramentos presentes no HIPPA e HITECH, o compartilhamento de dados com fontes de pagamento é baseado no consentimento do paciente. As regras para adoção do sistema de prontuário eletrônico e iniciativas posteriores para consolidar a interoperabilidade estão concentradas no ponto de cuidado e atenção ao paciente, ou seja,

---

87 United States Core Data for Interoperability (USCDI). Disponível em: <<https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi>>. Acesso em: 11 mar. 2022; The U.S. Core Data for Interoperability: A National Policy Journey. Disponível em: <https://www.centerfordigitalhealthinnovation.org/posts/the-us-core-data-for-interoperability-a-national-policy-journey>. Acesso em: 11 mar. 2022.

88 **ONC’s Cures Act Final Rule**. Disponível em: <<https://www.healthit.gov/curesrule/overview/about-oncs-cures-act-final-rule>>. Acesso em: 11 mar. 2022.

89 Confira o documento completo em: <https://www.govinfo.gov/content/pkg/FR-2020-05-01/pdf/2020-07419.pdf>.

envolve os profissionais de saúde e estabelecimentos de saúde, além de empresas fornecedoras de soluções de TI naquilo que for necessário para operacionalizar a interoperabilidade de dados. A interoperabilidade de prontuários não alcança as fontes pagadoras ou seguradoras de saúde, que, conforme os parâmetros do HIPAA e do HITECH devem se basear no consentimento dos pacientes. Seguradoras de saúde podem, portanto, ter acesso aos prontuários médicos e dados neles contidos desde que obtenham consentimento de seus beneficiários. Além disso podem, a partir de consentimento, ter acesso a outras fontes de dados de saúde, como aplicativos e *wearables* (dispositivos “vestíveis”) em programas desenvolvidos por seguradoras para promover e incentivar (inclusive com possibilidade de descontos) hábitos saudáveis, prevenção e atenção primária. A gestão do consentimento por meio dos aplicativos de TI, porém, tem sido objeto de críticas pelas associações médicas, como indicado a seguir.

Com relação ao uso para finalidade de pesquisa e políticas públicas de saúde, há a preocupação e esforço no sentido de desidentificação ou agregação de dados sem referência aos pacientes, muito embora haja críticas em relação às flexibilizações ao uso de dados nas políticas de combate à pandemia de COVID-19.

Mesmo com as medidas de preservação da privacidade para a interoperabilidade dos dados, restrita aos profissionais de saúde, estabelecimentos de saúde e aplicativos, organizações proeminentes, como a Associação Médica Americana, advertiram que, sem as devidas salvaguardas a nível federal, as novas regras de interoperabilidade poderiam expor as pessoas que compartilham seus diagnósticos e outros detalhes médicos íntimos com aplicações de consumidores. Os hospitais têm sido particularmente críticos, argumentando em uma declaração que a regra “*não protege as informações mais sensíveis dos consumidores sobre sua saúde pessoal*”.<sup>90</sup>

Como exposto no início deste relatório, a HIPAA se aplica a prestadores de serviços de saúde, seguradoras de saúde e terceiros que trabalham com eles, e atualmente, as grandes empresas de tecnologia são os terceiros com os quais os hospitais compartilham dados. Todavia, o que tornou evidente com exemplos recentes divulgados nacionalmente, as informações sobre saúde dos pacientes foram compartilhadas com e utilizadas por empresas de tecnologia para fins que não a promoção de saúde. Além disso, outra preocupação se refere ao fato de que empresas de tecnologia e empresas de aplicativos para smartphones que recebem dados de saúde diretamente de pacientes, médicos ou hospitais que os compartilham com base na autorização de um paciente não estão sujeitas à HIPAA.

A lacuna existente nas leis de privacidade pode se agravar à medida que as novas regras aumentam a capacidade dos pacientes - e de terceiros - de compartilhar dados. Alguns grupos compostos de entidades de saúde e outros interessados, como a *CARIN Alliance*, desenvolveram códigos de conduta voluntários para entidades não cobertas pela HIPAA, tais como aplicativos de terceiros, estabelecendo regras (voluntárias) para lidar com dados de assistência médica acessados via APIs.<sup>91</sup> Embora seja uma iniciativa

---

90 **Statement on ONC Final Rule | AHA.** Disponível em: <<https://www.aha.org/press-releases/2020-03-09-statement-onc-final-rule>>. Acesso em: 11 mar. 2022.

91 **Trust Framework and Code of Conduct. CARIN Alliance,** [s.d.]. Disponível em: <<https://www.carinalliance.com/our-work/trust-framework-and-code-of-conduct/>>. Acesso em: 11 mar. 2022.

que vai ao encontro da experiência internacional, sobretudo europeia, relativa à regulação setorial de novas tecnologias, a ausência de um órgão supervisor nos Estados Unidos torna o cumprimento das disposições dos códigos de conduta sujeito à mera voluntariedade das entidades.

As empresas de tecnologia e aplicativos de saúde são supervisionados principalmente pela Comissão Federal de Comércio (FTC), que se concentra principalmente na adesão das empresas às suas próprias políticas de privacidade. Os termos de acordo de serviços em sites de tecnologia e aplicativos de saúde, mesmo quando lidos pelos pacientes, geralmente são longos, opacos e de difícil compreensão, sendo que muitas vezes os pacientes não percebem que suas informações pessoais de saúde podem ser compartilhadas com anunciantes e comerciantes. A capacidade de atuação da FTC é apenas indireta e, como alguns argumentam, inadequada: a FTC deve provar após um abuso de privacidade de dados que as empresas de tecnologia e os desenvolvedores de aplicativos têm apresentado falsamente suas práticas de privacidade para que qualquer recurso legal possa ocorrer.

Até mesmo os reguladores federais de saúde reconhecem os riscos à privacidade apresentados pelas novas capacidades de compartilhamento de dados. Um infográfico sobre os direitos dos dados dos pacientes no site do ONC adverte: *“Tenha cuidado ao enviar suas informações de saúde para uma aplicação móvel”* porque os provedores de saúde *“não são mais responsáveis pela segurança de suas informações de saúde depois que elas são enviadas a terceiros”*<sup>92</sup>.

Ou seja, na visão dos críticos, o direcionamento do sistema para um controle de acesso pelos próprios pacientes, por meio autorizações de compartilhamento nos aplicativos de saúde pode expor os próprios pacientes a riscos, tendo em vista sua limitação para compreender a extensão desse compartilhamento, de modo que se defende modelo no qual o controle de acesso aos dados e seu compartilhamento deveria ficar restrito aos profissionais de saúde, hospitais e estabelecimentos de saúde, ao passo que outros usos por terceiros, empresas de TI ou seguradoras de saúde deveria se basear no consentimento explícito e informado dos pacientes.

### **2.8.5 Conclusões parciais sobre o sistema estadunidense**

Com base nas informações colhidas sistema de saúde norte-americano, especificamente sobre prontuários eletrônicos e interoperabilidade de bases de dados, podem-se extrair as seguintes conclusões:

- i) O sistema de saúde dos EUA é um sistema misto, que conta com seguradoras e prestadores de serviços de saúde públicos e privados, com e sem fins lucrativos, sendo o sistema com a menor ingerência Estatal entre os países analisados;
- ii) Questões referentes a privacidade e proteção de dados pessoais são abordadas de forma setorial e diferentes esferas, pois não há uma legislação central sobre a

---

92 Confira o documento em:

[https://www.healthit.gov/sites/default/files/YourHealthInformationYourRights\\_Infographic-Web.pdf](https://www.healthit.gov/sites/default/files/YourHealthInformationYourRights_Infographic-Web.pdf).

- matéria no país, como acontece na Europa, com o GDPR, ou no Brasil e Argentina, que contam com suas respectivas leis de proteção de dados pessoais;
- iii) A principal legislação que trata sobre dados relacionados à saúde é o Health Insurance and Portability and Accountability Act (HIPAA), de 1996 que tem como objetivo proteger as informações de saúde de indivíduos, mas também possibilitar o compartilhamento de informações entre prestadores de serviços de saúde para garantir um atendimento médico de qualidade;
  - iv) Desde maio de 2020, é obrigatório que as informações armazenadas nos registros eletrônicos de saúde (electronic health records, EHR) sejam compartilhadas, sempre no ponto de atenção ou cuidado, com aqueles que tenham o direito legal de acessá-las, o que se restringe aos próprios pacientes e a prestadores de serviços de saúde (fundamentalmente, médicos e estabelecimentos de saúde);
  - v) As informações obrigatoriamente compartilhadas compõem o que se chamou de “conjunto de dados centrais para interoperabilidade”, que deve incluir, além de informações demográficas (como raça, idade e sexo), as informações clínicas vitais do indivíduo (como alergias, tipo sanguíneo etc.).
  - vi) As regras para adoção do sistema de prontuário eletrônico e iniciativas posteriores para consolidar a interoperabilidade estão concentradas no cuidado e atenção ao paciente, ou seja, envolve os profissionais de saúde e estabelecimentos de saúde, além de empresas fornecedoras de soluções de TI naquilo que for necessário para operacionalizar a interoperabilidade de dados;
  - vii) O compartilhamento de dados com fontes de pagamento é baseado no consentimento do paciente, e a interoperabilidade de prontuários eletrônicos não alcança as fontes pagadoras ou seguradoras de saúde;

## 2.9 Argentina

### 2.9.1 O Sistema de Saúde na Argentina

O sistema de saúde argentino tem uma estrutura mista e descentralizada. Seu caráter misto corresponde ao fato de derivar receitas tanto do setor público quanto do privado. Embora seja descentralizada pela estrutura federal do país, que dá às províncias plena autonomia em saúde pública, elas são em grande parte responsáveis pela prestação de serviços de saúde.

O problema resultante é que as acentuadas diferenças na distribuição de renda se refletem diretamente no sistema de saúde, principalmente nos setores com menor poder aquisitivo que não têm outra opção a não ser recorrer à cobertura pública (nacional, provincial ou municipal) como sua principal fonte de atendimento.

Este modelo federal implica que o Estado Nacional fornece recursos para as províncias através de transferências (eventuais ou planejadas). Por sua vez, o Conselho Federal de Saúde, presidido pelo Ministro Nacional da Saúde, tem a tarefa e a responsabilidade de coordenar as agendas provinciais.

Este sistema é financiado através de uma variedade de meios. Por exemplo, o plano nacional de saúde depende de fontes que vão desde impostos e taxas cobradas pelas tesourarias nacionais, provinciais e municipais, até contribuições à seguridade social dos beneficiários e seus empregadores, que respondem por uma parcela significativa das receitas. Por sua vez, o sistema de seguro pré-pago é apoiado por pagamentos diretos ou compensações das famílias e, por sua vez, por pagamentos individuais para consultas, copagamentos etc.

Em paralelo ao esquema explicado acima, existe também um esquema de proteção financeira que depende das instituições de seguridade social, que estão divididas em três grupos: o Programa de Assistência Médica Integral (PAMI), que depende do Instituto Nacional de Serviços Sociais para Aposentados e Pensionistas (INSSJP); as vinte e quatro Obras Sociais Provinciais (OSPr) que dependem do emprego público em cada província; e, finalmente, as aproximadamente trezentas Obras Sociais Nacionais (OSN) que dependem normativamente da Superintendência Nacional de Seguros (SSN).

Estima-se que aproximadamente 33% da população faça uso de cobertura pública, e 10% contratem seguros privados. Os 57% restantes estão divididos entre um dos três blocos de previdência social (34% nos OSNs, 14% no OSPr e o restante no PAMI, especialmente aqueles com mais de 65 anos de idade).

Continuando com as estatísticas, com base nos números obtidos em 2015, estima-se que de cada 100 pesos (menos de US\$ 1 à taxa de câmbio oficial) investidos em saúde, 78,4% correspondem às contribuições dos sistemas de solidariedade, tanto públicos quanto previdenciários, e os 21,6% restantes são atribuídos ao pagamento direto privado, seja por meio de pagamentos sem juros (copagamentos, consultas diretas, medicamentos, etc.) ou por meio de desembolsos para pagamento de seguro de saúde pré-pago, em proporções muito semelhantes (51,8% e 48,2%, respectivamente).

Em termos de gastos públicos especificamente, as províncias são as principais contribuintes, respondendo por 62,6 por cento. O governo nacional contribui com 20,5 por cento e os 16,9 por cento restantes são fornecidos pelos municípios.

O percentual do Produto Interno Bruto (PIB) destinado à saúde é de aproximadamente 9,3%, um dos mais altos da região da América Latina.

## **2.9.2 Proteção da saúde e dos dados pessoais - Privacidade dos dados**

Em 2000, a Lei de Proteção de Dados Pessoais (Lei nº 25.326) foi aprovada na Argentina. Esta lei desempenha um papel fundamental nesse tema. O objetivo desta lei, como declarado em seu primeiro artigo, é a proteção integral dos dados pessoais registrados em arquivos, registros, bancos de dados ou outros meios técnicos de processamento de dados, públicos ou privados, destinados a fornecer informações, a fim de garantir o direito à honra e à privacidade dos indivíduos, bem como o acesso às informações registradas sobre eles. O mesmo artigo menciona sua origem constitucional, especificamente o artigo 43, em seu terceiro parágrafo, no que é conhecido como "habeas data", que, simplesmente explicado, é o direito dos cidadãos de retificar as informações que tanto o Estado como as entidades privadas possuem sobre eles.



Da mesma forma, o direito à saúde também corresponde a outros artigos da Constituição Nacional, como o artigo 42 “os consumidores de bens e serviços têm direito na relação de consumo à proteção de sua saúde, segurança e interesses econômicos (...)”, e mesmo com os diferentes tratados internacionais que, desde a reforma constitucional de 1994, têm hierarquia constitucional, após a introdução do novo artigo 75, parágrafo 22. É o caso de tratados como a Convenção Americana sobre Direitos Humanos, a Declaração Universal dos Direitos Humanos, o Pacto Internacional sobre Direitos Civis e Políticos ou a Declaração Americana dos Direitos e Deveres do Homem. Todos estes tratados mencionam de alguma forma o direito à saúde, reforçando assim sua proteção constitucional. Também deve ser feita menção especial ao Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais, que é considerado o tratado com as mais completas e abrangentes disposições sobre o direito à saúde dentro do sistema internacional de direitos humanos.

Com relação à Lei No. 25.326, é necessário estabelecer o que se entende por dados pessoais nessa lei. Referindo-se às definições dadas no Artigo 2, dados pessoais são “*informações de qualquer tipo relativas a pessoas físicas ou jurídicas que são determinadas ou determináveis*”. O citado artigo 2 também define dados sensíveis como “*dados pessoais que revelem origem racial e étnica, opiniões políticas, convicções religiosas, filosóficas ou morais, filiação sindical e informações relativas à saúde ou à vida sexual*”. A inclusão de informações sobre saúde nos dados classificados como sensíveis é digna de nota. Esta é uma caracterização que reafirma a importância da devida proteção das informações relacionadas à saúde, com tratamento particular ou especial.

O artigo 7 contém dois parágrafos com questões relevantes para nossa análise. Em primeiro lugar, é expressamente declarado que nenhuma pessoa pode ser obrigada a fornecer dados sensíveis. Em segundo lugar, e com relação aos dados sensíveis, a regra explica que estes só podem ser coletados e processados quando há razões de interesse geral autorizadas por lei. Uma exceção a esta última também é mencionada, afirmando que os dados sensíveis podem ser processados para fins estatísticos ou científicos, mas a exigência é que os sujeitos dos dados não possam ser identificados.

Finalmente, o Artigo 8, intitulado “Dados relativos à saúde”, prevê que os estabelecimentos de saúde públicos ou privados e os profissionais de ciências da saúde podem coletar e processar dados pessoais relativos à saúde física ou mental dos pacientes que os visitam ou que são ou foram tratados por eles, respeitando os princípios do sigilo profissional, entendido como uma forma de respeitar e garantir a privacidade dos pacientes.

No que diz respeito à relação dos dados decorrentes do prontuário médico de um paciente com a proteção de dados pessoais, o processamento desses dados relacionados à saúde deve responder a princípios básicos como o respeito à dignidade da pessoa e à autonomia da vontade do paciente.

### **2.9.3 O Sistema Nacional de Dados de Saúde: Registros médicos e a interoperabilidade dos dados médicos na Argentina**

O registro médico no sistema jurídico argentino é definido na Lei Nacional de Saúde Pública (Lei nº 26.529) como o documento cronológico, foliatizado e completo obrigatório

no qual são registradas todas as ações e/ou serviços prestados ao paciente pelos profissionais de saúde e auxiliares de saúde (artigo 12).

É um documento médico legal que registra de forma ordenada os dados relevantes sobre a saúde do paciente. O artigo 13 daquela lei incorpora a possibilidade de preparar dados médicos em meios magnéticos (registros médicos informatizados) e é decisivo em termos dos princípios que devem ser respeitados para garantir a inviolabilidade, segurança, confidencialidade e acessibilidade restrita daqueles dados sensíveis. Para tal fim, a adoção de acesso restrito foi regulamentada com os próprios códigos de identificação do titular ou qualquer outra técnica apropriada e suficiente para garantir a integridade das informações registradas.

Na jurisdição da Cidade Autônoma de Buenos Aires, os registros médicos são regulamentados pela Lei nº 5.669, que está conceitual e teoricamente de acordo com as disposições da Lei Nacional nº 26.529. O artigo 9 da lei descreve o Registro Sanitário Eletrônico como o documento digital e obrigatório contendo os serviços de saúde fornecidos ao paciente com a assinatura eletrônica ou digital da pessoa responsável.

A lei da província, ao contrário da legislação nacional, contemplou o Sistema Integrado de Registros de Saúde ("SIHCE"), estabelecendo um regime de interoperabilidade. Permite o armazenamento, gerenciamento e compartilhamento de informações documentadas entre diferentes estabelecimentos de saúde e/ou estabelecimentos de saúde da mesma jurisdição (públicos, previdência social ou privados, ou em consultórios privados). O SIHCE foi estabelecido para todos os habitantes que recebem cuidados de saúde na Cidade Autônoma de Buenos Aires. A implementação desse sistema implica que as instituições autorizadas compartilham informações e conhecimentos por meio do intercâmbio de dados entre seus próprios sistemas tecnológicos institucionais.

Em outras palavras, o SIHCE permite a cooperação e o intercâmbio de informações médicas dos pacientes (interoperabilidade dos dados médicos). Está previsto que *"todos os estabelecimentos de saúde localizados no território da CABA, sejam eles públicos, privados ou previdenciários, devem fornecer os meios necessários para a implementação do Sistema Integrado de Registros Eletrônicos de Saúde (SIHCE) e do Registro de Registros Eletrônicos de Saúde da CABA (RHCE)"* (Artigo 15) e que *"os estabelecimentos de saúde que prestam serviços no território da CABA, devem (...) gerar os meios para disponibilizar e compartilhar as informações, assim como as funcionalidades e funcionalidades para a interoperabilidade dos dados médicos"* (Artigo 15) e que *"os meios para disponibilizar e compartilhar as informações, assim como as funcionalidades e funcionalidades para a interoperabilidade dos dados médicos"* (Artigo 16)...*) gerar os meios para disponibilizar e compartilhar as informações, assim como as funcionalidades e soluções tecnológicas, entre aqueles que as requerem"* (Artigo 22.4).

Por outro lado, a Lei N°14.494 da Província de Buenos Aires estabeleceu um único sistema de registro médico eletrônico para cada pessoa, pelo qual um único registro médico é entendido como o conjunto de dados clínicos, sociais e administrativos relacionados à saúde de uma pessoa, processados através de computador ou meios telemáticos (Artigo 2).

Em nível nacional, existe a Lei de Saúde Pública N°26.529 acima mencionada e seu Decreto Regulamentar N°1089/2012, que regulamenta os direitos dos pacientes, os regis-

tros médicos e o consentimento informado do paciente.

Ao contrário do regime de interoperabilidade implementado pelo Governo da Cidade Autônoma de Buenos Aires, em nível nacional (Lei nº 26.529) e na Província de Buenos Aires (Lei nº 14.494), nenhum sistema similar foi regulamentado ou estabelecido para permitir a colaboração de informações médicas. Em outras palavras, um regime geral de interoperabilidade ao qual todos os agentes de saúde devem se conformar não foi regulamentado. A doutrina tem mencionado que, na prática, cada instituição de saúde pública ou privada digitalizou os registros médicos para seu próprio benefício sem cooperar com outros centros de saúde.

Portanto, pode-se concluir que na Argentina não existe um registro de saúde eletrônico unificado, mas apenas um único criado digitalmente dentro de cada estabelecimento de saúde público ou privado. Além disso, exceto na jurisdição da Cidade Autônoma de Buenos Aires, não há obrigação de compartilhar estes registros médicos entre os diferentes atores da saúde no resto do país.

#### **2.9.4 Compartilhamento de registros médicos com seguradoras de saúde**

Como indicado acima, na Argentina e em nível nacional, não há regulamentação específica sobre a interoperabilidade de dados médicos entre estabelecimentos de saúde públicos, de previdência social ou privados ou consultórios privados e terceiros.

Vale destacar os seguintes artigos das leis acima mencionadas que nos permitem concluir que a transferência das informações contidas na ficha médica depende da autorização expressa do titular da ficha médica. A propriedade inviolável do documento é sustentada pelos princípios e preceitos indicados a seguir, que devem ser rigorosamente respeitados devido à sensibilidade dos dados pessoais e sua proteção com origem constitucional.

No que diz respeito à propriedade das informações sanitárias, deve-se mencionar a mudança que ocorreu na Argentina. Antes da Lei 26.529 e de seu decreto regulamentar, havia consenso doutrinário que atribuía a propriedade da ficha médica ao estabelecimento, clínica ou médico particular. Isto foi baseado no fato de que são eles que possuem os conhecimentos técnicos necessários para poder elaborar tal documento. O paciente, por outro lado, era o proprietário dos dados contidos no prontuário médico. A lógica desta posição doutrinária surge da exigência legal de que o profissional de saúde mantenha o prontuário médico por um determinado período e garanta a possibilidade de acesso ao paciente.

Desde a entrada em vigor da Lei nº 26.529 (em 2009), o paciente é o proprietário do prontuário médico (artigo 14) e os estabelecimentos de atendimento e/ou hospitalares são os depositários do prontuário médico (exigência de custódia e guarda) e não os proprietários do documento. Os depositários são expressamente obrigados a implementar os recursos e meios necessários para impedir o acesso às informações contidas no prontuário médico por pessoas não autorizadas.

As pessoas autorizadas estão listadas no Artigo 19: o paciente e seu representante legal, cônjuge ou parceiro (...) e médicos/profissionais de saúde. Com relação àqueles que

não são titulares do documento, fica estabelecido que a autorização expressa do titular é necessária para solicitar e ter acesso a seus registros médicos. Ou seja, terceiros, mesmo que sejam os mencionados no artigo 19 inc. b e c, também precisam da autorização expressa do paciente para poder ter acesso a ela.

A Lei de Saúde Pública foi regulamentada pelo Decreto n. 26.529/2012. O artigo 2(d) do regulamento enfatiza o direito do paciente de não ter sua documentação clínica divulgada sem sua autorização expressa. Exceto nos casos em que a lei ou outras leis assim o estipulem, quando há uma ordem judicial em contrário, ou para evitar um dano maior por razões de saúde pública. Caso contrário, não seria possível uma transferência direta entre instituições e terceiros que não são considerados prestadores de serviços de saúde (artigo 2º do Decreto nº 1089/2012). Um prestador de serviços de saúde é qualquer pessoa física ou jurídica que fornece serviços de cuidado à saúde para fins de promoção, prevenção, cuidado e reabilitação, o que abrange profissionais de saúde e estabelecimentos que promovam qualquer tipo de atendimento ou tratamento ao paciente. Ou seja, empresas de seguro saúde não estão abrangidas e precisam do consentimento informado do paciente para que possam acessar seus registros médicos.

Com relação aos princípios da Lei n. 5. 669 da Cidade Autônoma de Buenos Aires, o Artigo 7 determina que o SIHCE, os registros médicos eletrônicos e todas as informações de saúde coletadas, devem estar em conformidade com certos princípios de desempenho e operação garantidos. Além dos princípios estabelecidos na Lei de Proteção de Dados Pessoais (Nº 25.326 a nível nacional e Nº1 845 da Cidade Autônoma de Buenos Aires) e na Lei Nº 26.529. Com relação à autorização do paciente para o processamento de seus dados médicos, os princípios de acessibilidade, confidencialidade, privacidade e segurança são comprometidos.

Com relação ao primeiro, o acesso deve ser limitado pelo direito fundamental do paciente à privacidade. Em matéria de confidencialidade, os dados clínicos devem ser tratados com a máxima reserva. O que é de suma importância nesta definição é que os dados médicos do paciente não estão disponíveis e não podem ser revelados a indivíduos, entidades ou processos sem o devido consentimento informado.

Há duas exceções previstas pelo Decreto n.1089/2012 à obrigação de confidencialidade, que surgem do Artigo 4. Em primeiro lugar, quando, na opinião do profissional, a saúde pública e/ou a saúde ou integridade física de outra(s) pessoa(s) está/estão em risco, o profissional está isento do cumprimento desta obrigação, uma vez que o risco excede a situação pessoal. Por exemplo, quando há a possibilidade de que um passageiro vindo do exterior possa propagar uma doença que não está presente no país. Neste caso, a ordem de saúde pública da população prevalece como um interesse primordial.

A segunda exceção, mencionada no parágrafo 2, ocorre quando há necessidade de acesso a informações confidenciais a fim de realizar auditorias médicas ou de saúde ou para o trabalho de financiadores de assistência médica. A condição é que devem ser adotados mecanismos para salvaguardar a confidencialidade dos dados que são inerentes ao paciente, uma vez que eles são protegidos pelo sigilo médico. Vale mencionar que "os financiadores da saúde são as entidades que recebem recursos de saúde e gerenciam a compra de produtos e serviços médicos para atender a população coberta. Na seguridade social, estas entidades são as organizações de seguridade social (OS) e, na medicina privada, as empresas de medicina pré-paga".

O princípio da privacidade estabelece que os dados registrados no prontuário médico eletrônico são considerados dados pessoais, confidenciais e sensíveis (o paciente tem o direito de conhecê-los a todo momento). Além disso, sua confidencialidade, integridade e disponibilidade (segurança) devem ser preservadas, evitando o uso ilícito ou ilegítimo que possa prejudicar os interesses ou direitos do detentor das informações de saúde (art. 22.3).

Do acima exposto, conclui-se que com a autorização do paciente, qualquer pessoa (física e/ou jurídica) pode acessar sua história clínica. Isto assegura a confidencialidade dos dados sensíveis e o respeito pela dignidade da pessoa, com o consentimento informado do proprietário é possível obter, classificar, utilizar, gerenciar, armazenar e transmitir informações ou documentação clínica. As medidas de segurança implementadas nestes regulamentos são rigorosas devido à sensibilidade dos dados relacionados à saúde.

### **2.9.5 Conclusões parciais sobre o sistema argentino**

A partir do exposto sobre as particularidades do sistema de saúde argentino, levando-se em consideração as normativas sobre proteção de dados pessoais e demais legislações pertinentes, é possível concluir o seguinte:

- i) O sistema de saúde argentino tem uma estrutura mista e descentralizada, mas com participação estatal significativamente maior que a privada;
- ii) De acordo com a Lei de Proteção de Dados Pessoais (Lei nº 25.326) argentina, nenhuma pessoa pode ser obrigada a fornecer dados sensíveis, que só podem ser coletados e processados quando há razões de interesse geral autorizadas por lei (exceto nos casos de fins estatísticos ou científicos, desde que os dados sejam anonimizados);
- iii) O Artigo 8 da Lei, intitulado "Dados relativos à saúde", prevê que os estabelecimentos de saúde públicos ou privados e os profissionais de ciências da saúde podem coletar e processar dados pessoais relativos à saúde física ou mental dos pacientes que os visitam ou que são ou foram tratados por eles, respeitando os princípios do sigilo profissional, entendido como uma forma de respeitar e garantir a privacidade dos pacientes;
- iv) Assim, dados decorrentes do prontuário médico de um paciente estão sujeitos à legislação de proteção de dados pessoais, devendo ser observados princípios básicos como o respeito à dignidade da pessoa e à autonomia da vontade do paciente;
- v) O registro médico no sistema jurídico argentino é definido na Lei Nacional de Saúde Pública (Lei nº 26.529), que não prevê a centralização/interoperabilidade a nível nacional;
- vi) Na jurisdição da Capital, Buenos Aires, os registros médicos são regulamentados pela Lei nº 5.669, que está conceitual e teoricamente de acordo com as disposições da Lei Nacional nº 26.529, mas que, ao contrário da legislação nacional, contemplou o Sistema Integrado de Registros de Saúde, estabelecendo um regime de interoperabilidade dos dados médicos no âmbito da jurisdição;

- vii) Assim, pode-se afirmar que na Argentina não existe um registro de saúde eletrônico unificado, mas apenas um único criado digitalmente dentro de cada estabelecimento de saúde público ou privado, não havendo, exceto na jurisdição da Cidade Autônoma de Buenos Aires, obrigação de compartilhar estes registros médicos entre os diferentes atores da saúde no resto do país;
- viii) Também não há, a nível nacional (incluindo-se a jurisdição de Buenos Aires), regulamentação específica sobre o compartilhamento de dados médicos entre estabelecimentos de saúde públicos, de previdência social ou privados ou consultórios privados e terceiros;
- ix) A Lei de Saúde Pública foi regulamentada pelo Decreto No. 26.529/1089/2012, que enfatiza o direito do paciente de não ter sua documentação clínica divulgada sem sua autorização expressa;
- x) Além disso, o regulamento prevê expressamente que os dados registrados no prontuário médico eletrônico são considerados dados pessoais, confidenciais, de modo que sua confidencialidade, integridade e disponibilidade devem ser preservadas, evitando o uso ilícito ou ilegítimo que possa prejudicar os interesses ou direitos do detentor das informações de saúde;
- xi) Como compartilhamento de informações contidas na ficha médica depende da autorização expressa do titular da ficha médica, e as empresas de seguro saúde não estão abrangidas entre as instituições que podem ter acesso ao prontuário médico eletrônico, elas precisam do consentimento informado do paciente para que possam acessar seus registros médicos;
- xii) De maneira geral, é possível concluir que, com a autorização (consentimento) do paciente, qualquer pessoa (física e/ou jurídica) pode acessar seu histórico clínico, não havendo previsão legal que permita o acesso de empresas terceiras ou seguradoras de saúde aos dados sem a anuência do seu titular ou responsável/representante legal.

# 3. Compartilhamento de dados de saúde no Brasil

Este capítulo tem por objetivo apresentar os contornos gerais dos sistemas público e privado de saúde no Brasil, os quais, não obstante operem com regras, racionalidade e operadores específicos, partilham de alguns conceitos em comum, como o de *serviços de saúde*, conceito chave na análise deste relatório.

Também será revisada a legislação setorial que dispõe sobre as atividades de compartilhamento de dados de beneficiários, titulares de dados pessoais protegidos pela LGPD, pelos agentes que compõem de cadeia de saúde suplementar, detalhando os objetivos e exatos limites da regulação da ANS ao determinar a interoperabilidade entre os diferentes Sistemas de Informação de Saúde.

## 3.1 Modelo de assistência à saúde no Brasil

O modelo brasileiro de atenção e assistência à saúde tal qual hoje estruturado, teve sua origem com a promulgação da Constituição Federal de 1988, que define a saúde como um direito fundamental, oponível ao Estado, de acesso gratuito, universal e igualitário a todos os cidadãos, que deverá ser prestado diretamente pelo Poder Público, sem prejuízo de seu exercício por agentes econômicos, em regime privado. Desse modo,

convivem no Brasil dois subsistemas específicos com fontes de financiamento, normas e *players* distintos: o sistema público, representado pelo Sistema Único de Saúde – SUS, e o sistema de saúde privado, quase que completamente representado pelo mercado de saúde suplementar.

O Sistema Único de Saúde (SUS), na forma da Constituição Federal, é um sistema universal de saúde com financiamento público e participação de todos os entes da federação, gestão pública, única, com integração e articulação entre as diferentes esferas e a prestação de assistência, por meio de serviços de rede própria de municípios, estados e União, de serviços públicos de outras áreas de governo e de serviços de saúde privados contratados ou conveniados<sup>93</sup>. Nesse modelo, o atendimento de saúde compete aos Municípios e aos Estados, ficando a União com as funções de planejamento, fiscalização e controle.

O subsistema privado, por sua vez, é dividido em dois subsetores: o liberal clássico e o de saúde suplementar. O subsistema liberal clássico é o composto por serviços particulares autônomos, caracterizados por clientela própria, em que os profissionais da saúde estabelecem diretamente as condições de tratamento para o paciente e sua remuneração, sem qualquer intermediação (*out of pocket expenses*).

A saúde suplementar, por sua vez, é composta pelos serviços de saúde financiados pelos planos e seguros de saúde aos quais os beneficiários são vinculados por um contrato coletivo ou individual. Nessa medida, os elos da saúde suplementar concatenam *fornecedores de insumos* (fabricantes de materiais médicos, equipamentos e medicamentos) que comercializam seus produtos aos *prestadores de serviços de saúde* (médicos, clínicas e hospitais) aos *pacientes* (usuários finais).

Os prestadores de serviços de saúde, compostos por médicos, clínicas, hospitais, laboratórios e estabelecimentos de medicina diagnóstica, recebem os insumos para criar a infraestrutura para atenção à saúde do beneficiário. São eles que exercem a atividade finalística do sistema de saúde suplementar, que é o atendimento direto ao paciente para prevenção, diagnóstico e tratamento.

Por sua vez, a Lei Federal n. 9.656, de 3 de junho de 1998, que dispõe sobre os planos e seguros privados de assistência à saúde, define operadoras de planos privados de assistência à saúde (“OPSs”) como toda e qualquer pessoa jurídica de direito privado, independente da forma jurídica de sua constituição, que ofereça planos de assistência à saúde mediante contraprestações pecuniárias, para acesso e atendimento a profissionais

---

93 Constituição Federal

Art. 199, parágrafo único. As instituições privadas poderão participar do Sistema Único de Saúde, segundo diretrizes deste, mediante contrato de direito público ou convênio tendo preferência as entidades filantrópicas e as sem fins lucrativos.

Lei n. 8.080/1990

Art. 24. Quando as suas disponibilidades forem insuficientes para garantir a cobertura assistencial à população de uma determinada área, o Sistema Único de Saúde (SUS) poderá recorrer aos serviços ofertados pela iniciativa privada. Parágrafo único. A participação complementar dos serviços privados será formalizada mediante contrato ou convênio, observadas, a respeito, as normas de direito público.



ou serviços de saúde integrantes de rede própria ou credenciada, contratada ou referenciada, visando à assistência médica, hospitalar e odontológica do beneficiário.

O relacionamento entre prestadores de serviços de saúde e operadoras de planos de assistência à saúde é definido por contratos escritos que definem o credenciamento do médico ou do estabelecimento de saúde à rede de serviços da OPS. O médico e o estabelecimento de saúde, conveniados a um determinado plano de saúde, possuem como interesse atender aos pacientes da carteira daquele determinado plano. A OPS, por seu lado, tem como interesse ampliar sua rede credenciada de médicos e estabelecimentos de saúde para ser capaz de atrair o máximo possível de beneficiários, tendo em vista que a maior opção é percebida pelo beneficiário como um valor si. Importante destacar que os usuários finais não são "pacientes" das OPSs, mas apenas beneficiários de uma relação de intermediação de pagamento prestados pelos hospitais, clínicas e profissionais de saúde.

Os serviços de saúde, cujas atividades são subdivididas em atividades de atendimento hospitalar, atenção ambulatorial e atividades de diagnósticos e terapêuticas, e as operadoras de planos de assistência à saúde, definidas como atividades de seguro à saúde e plano de saúde, está bem clara na legislação tributária, ao definir os respectivos CNAEs das atividades.

## Descrição dos Códigos Nacionais de Atividades Econômicas (CNAE)

CNAE	ATIVIDADE	DETALHAMENTO
8610-1	ATIVIDADES DE ATENDIMENTO HOSPITALAR	Esta atividade compreende os serviços de internação de curta ou longa duração prestados a pacientes realizados em hospitais gerais e especializados, hospitais universitários, maternidades, hospitais psiquiátricos, centros de medicina preventiva e outras instituições de saúde com internação, incluindo-se os hospitais militares e os hospitais de centros penitenciários. Essas atividades são realizadas sob a supervisão direta de médicos e incluem: serviços de médicos, serviços de laboratório, radiológicos e anestesiológicos, serviços de centros cirúrgicos, atividades exercidas em unidades de hospitais preparadas para atendimento a urgências e atividades exercidas em prontos-socorros com assistência 24 horas e com leitos de observação. Fazem parte dessa atividade, também, os serviços farmacêuticos, de alimentação e outros serviços prestados em hospitais, os serviços prestados pelas unidades mistas de saúde, que são compostas por um centro de saúde e uma unidade de internação com características de hospital local de pequeno porte, sob administração única, e as atividades dos navios-hospitais e as atividades de centros de parto

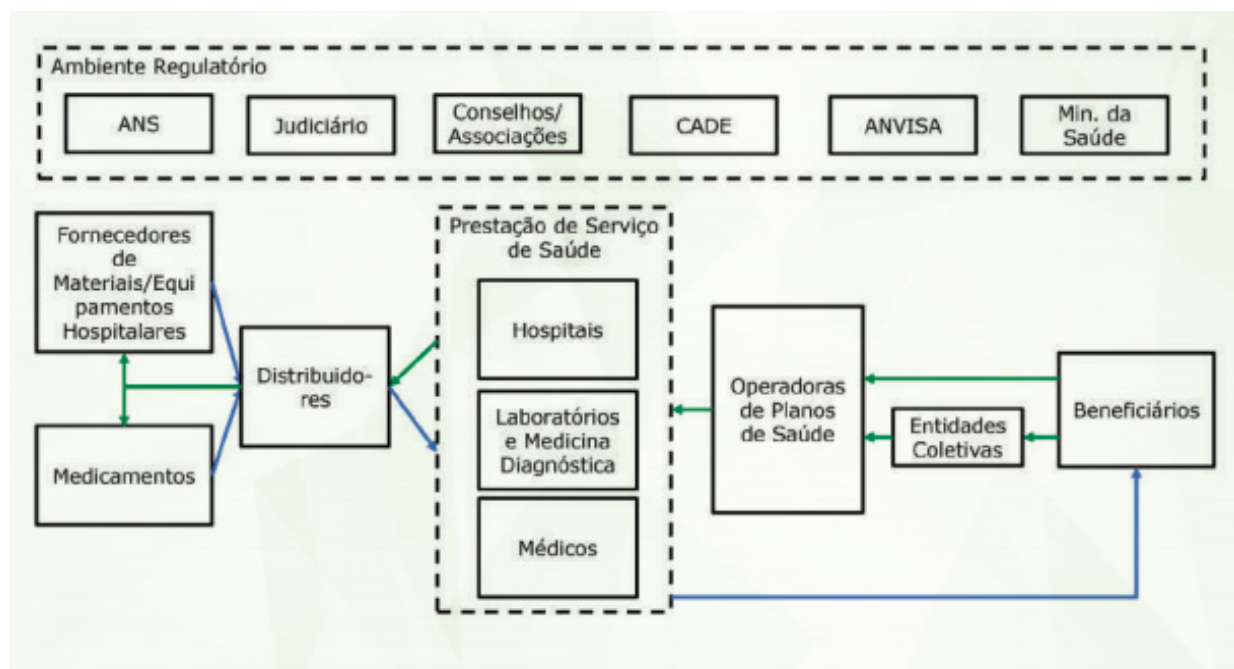
8630-5	<p>ATIVIDADES DE ATENÇÃO AMBULATORIAL EXECUTADAS POR MÉDICOS E ODONTÓLOGOS</p>	<p>Essa classe compreende as atividades de consultas e tratamento médico prestadas a pacientes que não estão sob regime de internação, como: consultórios, ambulatórios, postos de assistência médica, clínicas médicas especializadas ou não, policlínicas, consultórios privados em hospitais, clínicas de empresas, bem como realizadas no domicílio do paciente. Igualmente compreende as atividades dessa classe as unidades móveis fluviais equipadas apenas de consultório médico e sem leitos para internação, as atividades de consultas e tratamento odontológico exercidas em consultórios privados, ambulatórios, clínicas odontológicas, consultórios odontológicos em hospitais e em clínicas de empresas, bem como no domicílio do paciente, assim como os serviços de vacinação e imunização humana, a reprodução humana assistida, quando realizadas em unidades independentes de estabelecimentos hospitalares, as atividades prestadas por médicos autônomos ou constituídos como empresas individuais e que exercem a profissão em consultórios de terceiros ou em unidades hospitalares. Complementam as atividades dessa classe os postos de saúde pública, as unidades móveis terrestres equipadas de consultório odontológico e as unidades móveis fluviais equipadas de consultório odontológico.</p>
--------	--	--

8640-2	<p align="center"><b>ATIVIDADES DE SERVIÇOS DE COMPLEMENTAÇÃO DIAGNÓSTICA E TERAPÊUTICA</b></p>	<p>Fazem parte desta classe as seguintes atividades: • as atividades dos laboratórios de anatomia patológica e citológica, tais como: » exame citológico; » exame citopatológico; e » exame histopatológico. • as atividades dos laboratórios de análises clínicas; • os serviços de hemodiálise e diálise peritoneal; • os serviços de tomografia; • os serviços de radiodiagnóstico, tais como: » radiologia médica e odontológica; » densitometria óssea; » hemodinâmica; » medicina nuclear; » mamografia; e » fluoroscopia. • os serviços que realizam exames de ressonância magnética; • os serviços que realizam exames de ultrassonografia; • os serviços de diagnóstico por registro gráfico – ECG, EEG, polissonografia, audiometria e outros serviços de diagnóstico por registros gráficos; • os serviços de diagnóstico por métodos ópticos, tais como as endoscopias digestivas e respiratórias e outros exames análogos; • os serviços que realizam quimioterapia; • os serviços que realizam radioterapia; • os serviços prestados por hemocentros, núcleos de hemoterapia, unidades de coleta e transfusão, unidades de coleta de sangue, centrais de triagem laboratorial de doadores, agências transfusionais e demais serviços de hemoterapia; • os serviços de litotripsia; • as atividades dos bancos de células e tecidos humanos e dos bancos de ossos, quando realizadas em unidades independentes de hospitais; • os exames de função pulmonar, tais como a espirometria e a oxigenoterapia; • os outros serviços de complementação diagnóstica e terapêutica não especificados anteriormente; • as atividades de unidades móveis terrestres equipadas apenas de laboratório de análises clínicas, com pessoal especializado, sem fornecimento de consultas médicas; • as atividades de unidades móveis terrestres equipadas apenas de laboratório radiológico, com pessoal especializado, sem fornecimento de consultas médicas; e • os postos de coleta de laboratórios de análises clínicas</p>
6520-1	<p align="center"><b>SEGUROS-SAÚDE</b></p>	<p>Esta classe compreende o seguro-saúde, isto é, planos de seguro que garantem aos segurados a cobertura de despesas médico-hospitalares. A seguradora poderá pagar diretamente aos profissionais e organizações médico-hospitalares credenciados que prestaram os serviços, ou efetuar o reembolso ao próprio segurado. São operados por companhias seguradoras.</p>
6550-2	<p align="center"><b>PLANOS DE SAÚDE</b></p>	<p>Essa classe compreende os planos com coberturas de riscos, parcial ou total, na área de assistência à saúde (médico-hospitalar e odontológica) comercializados pelas empresas de medicina de grupo, cooperativas médicas, sistemas de autogestão e empresas de administração.</p>

Fonte: Confederação Nacional de Saúde. Radiografia Da Tributação Do Setor De Saúde<sup>94</sup>.

Por sua vez, a figura abaixo apresenta um esquema resumido das relações entre diferentes agentes e submercados no mercado de saúde suplementar. Vê-se no diagrama a relação entre os prestadores de serviço de saúde, operadoras de planos de saúde e beneficiários, além dos diversos órgãos e entidades governamentais responsáveis pela regulação do setor de saúde suplementar, sendo sobretudo relevante para esta análise o papel da ANS e do CADE.

## Mapa da cadeia produtiva da saúde suplementar



Fonte: Azevedo et. al, 2016.

O modelo de regulação do setor de saúde suplementar brasileiro é recente, tendo sido gestado após mais de 30 anos de operações privadas sem a edição de um marco regulatório disciplinador. O primeiro normativo do setor de saúde suplementar foi a Lei n. 9.656/98, que dispõe sobre os planos e seguros privados de assistência à saúde e define as relações entre operadoras, produtos e seus beneficiários. Antes da publicação daquela Lei, os consumidores somente podiam recorrer ao Código de Defesa do Consumidor e aos PROCONs no caso de conflitos com operadoras e planos de saúde.

Posteriormente, em 28 de janeiro de 2000, foi publicada a Lei n. 9.961, que criou Agência Nacional de Saúde Suplementar (ANS), autarquia sob regime especial vinculada ao Ministério da Saúde que tem, nos termos do art. 3º da Lei, por finalidade institucional promover a defesa do interesse público na assistência suplementar à saúde, regulando as operadoras setoriais, inclusive quanto às suas relações com prestadores e consumidores, contribuindo para o desenvolvimento das ações de saúde no País.

A ação reguladora da ANS é fundamentada no pressuposto de que o setor da assistência à saúde é imperfeito, com assimetrias profundas entre as OPSs e beneficiários, e não pode ser relegado tão-somente às forças de mercado. Com isso, o bom funcionamento do setor para a persecução dos valores constitucionais demanda regras para garantir a prevalência do interesse público e, também, para equilibrar a relação entre consumidores, operadoras e prestadores de serviços de saúde.

Tratando-se de um setor complexo, com a atuação de diversos atores, a ANS foi definindo, a partir da legislação em vigor, regras para a contratação dos serviços médicos pelas OPS e para a circulação, conexão e coordenação dos dados pelos diversos agentes envolvidos na contraprestação a serviço contratado, normas que dialogam com a legislação de proteção de dados em vigor a partir da publicação da LGPD e suas alterações supervenientes (sobretudo com a superveniência da Lei n. 13.853/2019). Os aspectos relativos ao compartilhamento de dados entre os agentes do mercado de saúde suplementar serão examinados em tópico próprio.

## **3.2 Compartilhamento de informações de saúde na saúde suplementar**

### **3.2.1 A Coleta de Dados de Saúde e a gestão de pagamento na saúde suplementar**

A coleta de dados pessoais é inerente ao atendimento por profissionais de saúde ou estabelecimentos de saúde. O cuidado ao paciente depende integralmente da correta identificação do paciente e avaliação de informações sobre seu histórico e estado atual saúde, bem como de sintomas manifestados que motivaram a busca por atenção. No ingresso do paciente no ambiente hospitalar, há a necessidade de identificação e registro dos dados e procedimentos do paciente para finalidades administrativas. Dentre os objetivos desta coleta estão a verificação de existência de seguro saúde (quando aplicável), a identificação de prontuário anterior, controle de entrada e saída de pacientes e visitantes, dentre outros. A identificação correta é também importante para direcionar o atendimento por profissionais de saúde no momento do tratamento.

Posteriormente, o paciente é encaminhado à triagem e anamnese, que será realizada por profissional de saúde. A partir deste momento informações de saúde passam a ser coletadas e inseridas no prontuário do paciente. É possível que o caso requeira a solicitação de exames laboratoriais e/ou de imagem, os quais também serão inseridos no prontuário, ou seja, tanto sua solicitação quanto, os resultados obtidos em cada um.

A continuidade, pode haver a prescrição de medicamentos, indicação de retorno, internação, com diversas evoluções possíveis. Todas estas etapas, sem exceção, são registradas em prontuário, motivo pelo qual os dados ali contidos, mais que “meramente” dados de saúde, são de enorme densidade e revelam detalhes bastante sensíveis a respeito do titular.

Desde a entrada do paciente coberto por uma OPS no estabelecimento de saúde, há a necessidade de compartilhamento de alguns dados com a seguradora necessários para que sejam realizados os reembolsos ou custeio do atendimento realizado no estabelecimento. Assim, há a necessidade de identificação correta do paciente segurado e indicação dos procedimentos realizados, que serão remunerados ou reembolsados pela seguradora.

Essas informações são necessárias para o fluxo de obrigações decorrente da seguinte estrutura de contratos:

- i) A OPS celebra contrato de plano de saúde com o beneficiário, obrigando-se a cobrir os custos dos procedimentos médicos especificados no contrato;
- ii) A OPS celebra um contrato de credenciamento com os prestadores de serviços de saúde por meio do qual estes se obrigam a atender o grupo de vidas da OPS nas condições estabelecidas no contrato;

- iii) Prestadores de serviços de saúde celebram contratos de prestação de serviços com os pacientes, para atendimento de consultas médicas, internações, medicina diagnóstica, dentre outros.

Assim, para o cumprimento e execução do contrato é necessária a identificação do paciente e de seu plano de saúde com as coberturas já determinadas e a indicação do procedimento coberto pelo plano. Não é papel da seguradora, nessa estrutura contratual, avaliar o mérito do procedimento (exame, consulta, intervenção cirúrgica etc.), que é de responsabilidade do profissional de saúde. Portanto, não é necessário indicar resultados exames ou avaliações do estado de saúde, dados do histórico de saúde do paciente ou qualquer elemento direcionado a justificar a pertinência do tratamento para a execução do contrato com a OPS nesta etapa.

Por outro lado, quando uma unidade hospitalar ou estabelecimento de saúde presta serviços para determinada OPS, o seu credenciamento e relação contratual pressupõe a lealdade quanto as faturas encaminhadas, havendo dispositivos contratuais que asseguram o direito das OPSs de verificar as contas enviadas, como forma de garantir a idoneidade das cobranças realizadas. Trata-se da possibilidade de auditoria, pela OPS dos procedimentos relativos às contas encaminhadas para pagamento.

De maneira amostral ou não direcionada a pacientes específicos, os auditores dos seguros de saúde acessam prontuários médicos para garantir que os procedimentos executados são cabíveis para os casos ali narrados e que foram de fato executados. Esta análise é realizada por auditores médicos e tem como finalidade única garantir a pertinência da intervenção específica que gerou o custo para remuneração para OPS. Todos estes acessos, contudo, costumam ser feitos *in loco* e de maneira compartimentada (ou seja, sem acesso direto a uma base centralizada de informações. Assim, há a garantia de que as informações não trafegarão desnecessariamente. Dado que o objetivo da auditoria é garantir a correspondência entre as cobranças, os procedimentos, e a necessidade destes últimos, basta à seguradora a certificação do médico auditor de que as informações por ele analisadas são adequadas. Assim, por ser médico, tem a obrigação legal de guardar sob sigilo as informações que porventura tenha acesso na atividade de auditoria.

Este modelo garante às seguradoras a possibilidade de verificar a adequação das contas que lhes são apresentadas e glosá-las, quando for o caso. Uma vez que o médico auditor, contudo, garante que as informações estão todas compatíveis, não há transferência dos dados analisados à seguradora, tão somente uma indicação de aceite das contas e/ou inclusão de glosas necessárias. Enquanto este modelo cumpre perfeitamente às necessidades de faturamento e verificação de fraude por parte das seguradoras, impede-as de ter acesso direto aos dados de saúde de cada segurado.

Esse fluxo de informações é regulado em pormenores pela ANS, de modo a garantir a execução da finalidade dos contratos de prestação de serviços de saúde e de cobertura dos seus custos, com a proteção dos interesses do paciente (dentre eles, o atendimento de qualidade e a preservação de sua privacidade).

Com efeito, desde sua criação, que retoma ao ano 2000, a ANS foi definindo regras para a contratação dos serviços médicos pelas OPS e para a circulação, conexão e coordenação dos dados pelos diversos agentes envolvidos na cadeia da saúde suplementar.

No que mais interessa à presente análise, nos termos de sua lei de criação, a Agência possui competência para *fiscalizar* os operadores e prestadores de serviços, mediante o controle e a avaliação de aspectos concernentes à garantia de acesso, manutenção e qualidade dos serviços prestados, direta ou indiretamente, pelas OPS (art. 4º, XXIV), e para *proteger* os interesses do consumidor de serviços privados de assistência à saúde, zelando pela qualidade dos serviços de assistência à saúde no âmbito da assistência à saúde suplementar (art. 4º, XXXVII).

Para atendimento a estas atribuições finalísticas, a Lei atribui à ANS poderes para requisitar o fornecimento de informações às operadoras de planos privados de assistência à saúde, bem como da rede prestadora de serviços a elas credenciadas (art. 4º, XXXI, da Lei n. 9.961/2000) e para proceder à integração dessas informações com os bancos de dados do Sistema Único de Saúde (art. 4º, inciso XIX, da Lei n. 9.961/2000).

Em complemento, a Lei dos Planos de Saúde atribui às operadoras o dever de fornecer periodicamente à ANS todas as informações e estatísticas relativas às suas atividades, incluídas as de natureza cadastral, especialmente aquelas que permitam a identificação dos consumidores e de seus dependentes, incluindo seus nomes, inscrições no Cadastro de Pessoas Físicas e municípios onde residem.

Nessa medida, à ANS compete criar Sistemas de Informação em Saúde – SIS<sup>95</sup> que permitam a coleta, armazenamento, o processamento, a recuperação e a disseminação de informações na cadeia de saúde suplementar com o propósito de apoiar as funções operacionais, gerenciais e de tomada de decisão de interesse da saúde. Os principais Sistemas de Informação em Saúde da ANS são<sup>96</sup>:

- SIP – o Sistema de Informações de Produtos tem como finalidade acompanhar a assistência de serviços prestada aos beneficiários de planos de saúde.
- SIB – o Sistema de Informação de Beneficiários tem como finalidade acompanhar as informações cadastrais dos beneficiários nas bases de dados das operadoras na ANS.
- Sistema de Registro de Plano de Saúde (RPS), instrumento de envio das solicitações de registro de planos de saúde;
- Sistema de Documento de Informações Periódicas das Operadoras de Planos de Assistência à Saúde (DIOPS).

---

95 “Os Sistemas de Informação em Saúde (SIS) podem ser definidos como um conjunto de componentes inter-relacionados que coletam, processam, armazenam e distribuem a informação para apoiar o processo de tomada de decisão e auxiliar no controle das organizações de saúde. Assim, os sistemas de informação em saúde congregam um conjunto de dados, informações e conhecimento utilizados na área de saúde para sustentar o planejamento, o aperfeiçoamento e o processo decisório dos múltiplos profissionais da área da saúde envolvidos no atendimento aos pacientes e usuários do sistema de saúde.” (Cf. BARBOSA, Marcelo N. Possibilidades e limitações de uso das bases de dados do DATASUS no controle externo de políticas públicas de saúde no Brasil. TCU, Coletânea de Pós-Graduação, v.2 n.13 Auditoria do Setor Público).

96 Agência Nacional de Saúde Suplementar (Brasil). Atenção à saúde no setor suplementar: evolução e avanços do processo regulatório / Agência Nacional de Saúde Suplementar (Brasil). – Rio de Janeiro: ANS, 2009. 80 p.

A ANS ainda utiliza dados de outros SIS geridos no âmbito do Sistema Único de Saúde:

- Sistema de Comunicação de informações hospitalares e ambulatoriais do SUS (CIHA);
- Sistema do Cartão Nacional de Saúde (CNS);
- Sistema do Cadastro Nacional de Estabelecimentos de Saúde (SCNES). a ANS faz uso do Cadastro Nacional de Estabelecimentos de Saúde como identificador do prestador de serviço que atende aos planos privados de assistência à saúde, cujos registros são solicitados pelas operadoras do setor;
- Sistema de informações hospitalares do SUS (SIH). a ANS faz uso do Sistema de Comunicação de Internação Hospitalar para a verificação das ocorrências de todas as internações hospitalares no território nacional por meio de formulário padrão. O CIH foi criado em parceria com o Ministério da Saúde e com o Departamento de Informática do SUS (Datapus).<sup>97</sup>
- Sistema de informações ambulatoriais do SUS (SIA);
- Sistema de Mortalidade (SIM);
- Sistema de Nascidos Vivos (SINASC).

Para viabilizar os sistemas de informação sob sua gestão e a utilização de dados do SUS, a ANS desenvolveu o padrão de Troca de Informação em Saúde Suplementar – TISS para registro e intercâmbio de dados entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde. Em vigor desde 2012, com a publicação da Resolução Normativa n. 305/2012, a proposta da ANS utiliza padrões já existentes e disponíveis em outros bancos de dados e em SIS.

O padrão TISS define o modelo obrigatório para as trocas eletrônicas de dados de atenção à saúde dos beneficiários de planos, entre os agentes da saúde suplementar e tem por objetivo atingir a compatibilidade e interoperabilidade funcional e semântica entre os diversos sistemas independentes para fins de avaliação da assistência à saúde (caráter clínico, epidemiológico ou administrativo) e seus resultados, orientando o planejamento do setor. O Padrão TISS está organizado em cinco componentes: I - organizacional II - conteúdo e estrutura; III - representação de conceitos em saúde; IV - segurança e privacidade; e V - comunicação.

Nos termos da Resolução ANS n. 305/2012, o padrão TISS tem por objetivo:

- a) Padronizar as ações administrativas de verificação, solicitação, autorização, cobrança, demonstrativos de pagamento e recursos de glosas;
- b) Subsidiar as ações da ANS de avaliação e acompanhamento econômico, financeiro e assistencial das operadoras de planos privados de assistência à saúde;

---

97 Agência Nacional de Saúde Suplementar (Brasil). Atenção à saúde no setor suplementar: evolução e avanços do processo regulatório / Agência Nacional de Saúde Suplementar (Brasil). – Rio de Janeiro: ANS, 2009. 80 p.



- c) Compor o registro eletrônico dos dados de atenção à saúde dos beneficiários de planos privados de assistência à saúde.

O Padrão TISS abrange as trocas dos dados de atenção à saúde prestada ao beneficiário de plano privado de assistência à saúde gerados na rede de prestadores de serviços de saúde (contratada, referenciada ou credenciada, de forma direta ou indireta e a rede própria da operadora ou de seu grupo econômico) e a troca dos dados de atenção à saúde, gerados na modalidade reembolso das despesas assistenciais ao beneficiário.

### **3.2.1.1 Troca de informações entre prestadores de serviços de saúde e OPSs**

No que se refere à troca de informações entre operadoras e prestadores de serviços de saúde, o TISS estabelece a padronização dos seguintes processos:

- i) *Verificação de Elegibilidade*: Para sua execução, é necessária a identificação do beneficiário, bem como do prestador executante do procedimento.
- ii) *Autorização de procedimentos*: Para sua execução, é necessária a identificação do beneficiário, o prestador solicitante e executante e os procedimentos/ itens assistenciais para os quais está sendo solicitada a autorização. Podem ser necessários ainda esclarecimentos quanto à situação de saúde do beneficiário com vistas à autorização do procedimento solicitado.
- iii) *Comunicação de internação ou alta do beneficiário*: para sua execução, é necessária a identificação do beneficiário
- iv) *Cobrança de serviços de saúde*: Para sua execução, é necessária a identificação do beneficiário, o prestador solicitante e executante e os procedimentos/ itens assistenciais para os quais está sendo solicitada a autorização. Podem ser necessários ainda esclarecimentos quanto à situação de saúde do beneficiário com vistas à autorização do procedimento solicitado.
- v) *Demonstrativos de retorno*: Para sua execução, é necessário identificar o beneficiário, o prestador executante e os procedimentos/itens assistenciais envolvidos.
- vi) *Envio e recebimento de documentos*: São compartilhados os documentos que possam ser necessários para os processos de solicitação, autorização, cobrança e/ou recurso de glosa de procedimentos/itens assistenciais.
- vii) *Recurso de glosa*: Para sua execução é necessário identificar o beneficiário, o prestador executante e os procedimentos/itens assistenciais envolvidos. Podem ser necessários ainda esclarecimentos quanto à situação de saúde do beneficiário que deu origem ao atendimento realizado e recusado.
- viii) Comprovante presencial.

Dentre esses, é obrigatória a troca eletrônica de informações no padrão TISS para a cobrança de serviços de saúde, autorização de serviços, demonstrativos de retorno e recurso de glosas. A troca de informações relativas à verificação de elegibilidade, autorização de procedimentos, comunicação de internação ou alta do beneficiário e envio e recebimento de documentos pode ser realizada por meio físico e, exclusivamente nesta

hipótese, o uso do padrão TISS será opcional. Os processos padronizados para troca em papel conforme o contrato entre as partes são o comprovante presencial e a cobrança de serviços de saúde (Guia de Tratamento Odontológico - comprovante de atendimento).

### **3.2.1.2 Trocas de informações entre beneficiários e OPSs**

Entre operadoras e beneficiários, os processos de troca de informações padronizados são:

- i) Utilização de serviços: é a definição das informações que devem ser enviadas pela operadora aos beneficiários em cumprimento ao estabelecido pela RN n. 389/2015.
- ii) Informações acerca da negativa de autorização: é a definição do conjunto mínimo de informações que devem ser enviadas pela operadora aos beneficiários em cumprimento ao estabelecido pela RN n. 395/2016.
- iii) Informações sobre partos: é a definição do conjunto de informações que devem ser fornecidas pelas operadoras às beneficiárias em cumprimento ao estabelecido pela RN n. 368/2015.

As operadoras de planos privados de assistência à saúde e seus prestadores de serviços de saúde devem disponibilizar sem qualquer ônus, as informações de dados de atenção à saúde do Padrão TISS, solicitadas pelo beneficiário, por seu responsável legal ou ainda por terceiros formalmente autorizados por eles.

Nesse sentido, a Resolução Normativa nº 389, de 26 de novembro de 2015 dispõe sobre a transparência das informações no âmbito da saúde suplementar e estabelece a obrigatoriedade de as operadoras de planos privados de assistência à saúde disponibilizarem, em seus portais na internet, uma área específica e restrita para reunir informações individualizadas dos beneficiários, titulares e dependentes, assim como uma área destinada às empresas contratantes de planos coletivos. Nos termos da RN n. 389/2015, as operadoras deverão disponibilizar obrigatoriamente informações individualizadas relativas ao beneficiário por meio do Portal de Informações do Beneficiário da Saúde Suplementar – PIN-SS, que compreenderá dois componentes, o cadastral e o de utilização de serviços.

### 3.2.1.3 Trocas de informações entre OPSs e a ANS

Entre operadoras e ANS são padronizados os processos de troca de informações de dados de atenção à saúde dos beneficiários da saúde suplementar denominado *Envio de dados para a ANS* e de monitoramento da qualidade dos dados incorporados na ANS denominado *Monitoramento da qualidade dos dados incorporados na ANS*. Para tanto, é necessário identificar o beneficiário, o prestador solicitante e executante e os procedimentos/itens assistenciais envolvidos. Podem ser enviados, ainda, dados sobre a situação de saúde do beneficiário.<sup>98</sup>

Vale ressaltar que o Padrão TISS possui o componente de segurança e privacidade, que estabelece os requisitos de proteção dos dados de atenção à saúde com o objetivo de assegurar o direito individual ao sigilo, à privacidade e à confidencialidade dos dados de atenção à saúde e observa legislação vigente relativa ao sigilo profissional (art. 14 da RN 305/2012).

A partir deste panorama é possível afirmar que o compartilhamento de informações entre prestadores de serviços de saúde e OPS é fortemente regulado pela ANS por meio das especificações do padrão TISS, na medida que são definidos pela regulação os dados que devem ser compartilhados para viabilizar todos os procedimentos para o atendimento de saúde ao beneficiário.

## 3.3 Bases legais para o compartilhamento de dados de saúde entre estabelecimentos de saúde e Operadoras de Planos de Saúde conforme a Lei Geral de Proteção de Dados

### 3.3.1 Bases Legais autorizadas de tratamento conforme a LGPD

A privacidade de um paciente e o sigilo quanto a sua condição de saúde são elementos fundamentais da prática médica e dos demais profissionais da saúde. Não por acaso, o Código de Ética Médica<sup>99</sup> estabelece, dentre outras questões, o dever de sigilo médico-paciente nos seguintes termos: *‘Capítulo I – Princípios Fundamentais: [...] XI – O médico guardará sigilo a respeito das informações de que detenha conhecimento no desempenho de suas funções, com exceção dos casos previstos em lei’*.

Assim, o setor da saúde sempre esteve permeado pelo sigilo médico e, consequentemente, pela necessidade de cuidado com a divulgação e o compartilhamento de informações, buscando o melhor tratamento para os pacientes e, quando necessário, seu consentimento no compartilhamento de suas informações e na prática de procedimentos. Assim, se de um lado a coleta de informações para o tratamento do paciente é inerente à relação

98 Padrão TISS - Componente Organizacional – fevereiro de 2022. Disponível em: [https://www.gov.br/ans/pt-br/arquivos/assuntos/prestadores/padrao-para-troca-de-informacao-de-saude-suplementar-tiss/padrao-tiss/PadroTISS\\_ComponenteOrganizacional\\_202202.pdf](https://www.gov.br/ans/pt-br/arquivos/assuntos/prestadores/padrao-para-troca-de-informacao-de-saude-suplementar-tiss/padrao-tiss/PadroTISS_ComponenteOrganizacional_202202.pdf)

99 BRASIL, Resolução nº 2.217, de 27 de setembro de 2018 do Conselho Federal de Medicina (CFM). Aprova o Código de Ética Médica. Disponível em: <https://portal.cfm.org.br/images/PDF/cem2019.pdf> Acesso em: 17 fev. 2022.

médico-paciente, sendo necessário para a prestação do serviço médico na consecução de seus fins de cuidado e bem-estar do paciente, de outro, para o compartilhamento dessas informações com terceiros, rege a máxima de consentimento pelo paciente, devendo o médico guardar absoluto sigilo e não expor as informações de que veio a tomar conhecimento sobre o paciente no exercício de sua profissão.

Com a informatização dos serviços de saúde, a ética médica se propaga inclusive para os profissionais de informática em saúde para que o sistema sócio-técnico que lida com as informações dos pacientes assegure o sigilo. Assim, o Código de Ética da Associação Internacional de Informática Médica para Profissionais de Informática em Saúde (IMIA) estabelece que esses profissionais devem assegurar que os meios técnicos apropriados sejam adotados, de modo que prontuários ou registros eletrônicos sejam estabelecidos ou compartilhados por meios de transmissão somente com o consentimento voluntário, competente e informado dos pacientes aos quais esses registros se referem.

Nesse passo, ao proteger a autonomia do paciente quanto ao compartilhamento das informações, a ética médica e da informática médica dão um passo adicional ao resguardo, para adentrar na proteção dos dados pessoais dos pacientes em nome de sua *autodeterminação informativa*, que, ao lado da proteção à privacidade, é o princípio basilar da Lei Geral de Proteção de Dados Pessoais brasileira, Lei 13.709/2018, conforme indicado em seu art. 2º, inc. II.

O conceito de autodeterminação informativa e toda a construção da legislação de proteção de dados não se reduz à noção de sigilo. Possui uma dimensão dinâmica que vai muito além de um direito de defesa, que postularia um espaço privado de informações a não ser invadido e garantido pelo Estado.<sup>100</sup> A proteção de dados consiste, na verdade, em reforçar duas atribuições do indivíduo no novo cenário da sociedade da informação: (i) a transparência por parte da Administração e do setor privado sobre o uso de dados pessoais por eles detidos; (ii) colocar o indivíduo em posição ativa e dinâmica na relação com seus dados e informações perante o Estado e a iniciativa privada.<sup>101</sup>

E o mecanismo primordial adotado pela legislação de proteção de dados, arraigada no conceito de autodeterminação informacional, está no *princípio de finalidade*, que como previsto no art. 6º, inc. I da LGPD, consiste na “*realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades*”.

Trata-se de vincular e restringir a aplicação de qualquer informação derivada do processamento de dados pessoais ao objetivo que justificou sua coleta. Essa coleta deve ser legítima, ou seja, ter uma base autorizadora reconhecida pela lei para o tratamento de dados. Reconhece-se, assim, como fundamento legítimo para o tratamento, o consentimento que delimite seu escopo, o exercício de competência legal com objeto determina-

---

100 Para a forma clássica sobre o conceito de direitos de defesa ver Gertrude Lübke-Wolf, *Die Grundrechte als Eingriff-sabwehrrechte*, Baden-Badenn 1998. Sobre a crítica a concepção de direito fundamental de defesa frente ao Estado na proteção de dados ver Karl-Heinz Ladeur, “*Datenschutz - vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken. Zur objektiv-rechtlichen Dimension*” des Datenschutzes, DuD 2000, p. 12 ss.

101 Conforme anota a decisão, as pessoas têm “o poder, em princípio, de determinar por si próprias a atribuição e a utilização dos seus dados pessoais”. (Tradução livre) BVerfGE 65, 1.

do, a necessidade para prestação de serviço ou execução de contrato especificado etc. Em todo e qualquer caso, a justificativa original da coleta é que determina os limites do processamento, do emprego e da transmissão de informações dele extraídas. Por conseguinte, o tratamento de dados só pode ter lugar no âmbito de um objetivo definido, claro e legítimo. Em particular, o processamento para fins abertos ou desconhecidos é vedado pelo princípio da finalidade.<sup>102</sup> Além disso, a reutilização dos dados, com um tratamento distinto daquele que justificou a coleta necessita também de uma base autorizadora. Vale dizer, não só o tratamento original onde ocorre a coleta necessita de base legal, como também a sua reutilização, pelo mesmo, ou outro agente de tratamento necessita estar legitimado por base legal autorizadora prevista na lei.

Para os propósitos desse trabalho, considerando que a coleta e uso para o atendimento médico é uma forma de tratamento, ao passo que o compartilhamento dos dados médicos com terceiro, consiste em uma reutilização dos dados para outra finalidade, o compartilhamento também necessita de base legal.

Outro princípio fundamental para a aplicação e interpretação da LGPD é o da necessidade (art. 6º, III), consistente na *“limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados”*. Ou seja, o tratamento, além de ter uma base legítima, deve se ater ao estritamente necessário para cumprir a finalidade da coleta. Isso significa não só uma restrição aos diferentes tipos de tratamento, como à própria coleta e armazenamento dos dados pessoais, de modo que, se a aplicação pretendida não é necessária para atender à finalidade pretendida, a própria coleta não se justifica.

### **3.3.2 Possíveis bases legais para o compartilhamento de dados entre estabelecimentos de saúde e OPSs**

Os dados de saúde são explicitamente indicados pela LGPD como dados sensíveis (art. 5º, inc. II) e que, portanto, merecem um cuidado especial, com maiores restrições em relação às bases legais para seu tratamento. Assim é que a LGPD restringe a legitimidade do tratamento primordialmente ao consentimento do titular (art. 11, inc. I), mas admite exceções, apenas naquelas hipóteses em que o tratamento for *indispensável* – e aqui novamente se reforça o *princípio de necessidade*) –, para as seguintes finalidades:

- a) *cumprimento de obrigação legal ou regulatória;*
- b) *tratamento de dados compartilhados necessários a execução de políticas públicas previstas em lei;*
- c) *realização de estudos por órgãos de pesquisa, utilizando-se a anonimização, quando possível;*

---

102 Sobre o assunto ver os casos elencados de coleta de dados sem finalidade na diretiva europeia RL 2006/24/EG e as decisões do tribunal europeu sobre o assunto EuGH, C-293/12 e C-594/12. Na doutrina, Spiros Simitis: *Die Vorratsspeicherung – ein unverändert zweifelhaftes Privileg*, In: Neue Juristische Wochenschrift, 2014, p. 2158 ss.

- d) exercício regular de direitos, inclusive em contrato ou processo judicial ou arbitral
- e) proteção à vida ou incolumidade física do titular ou terceiro
- f) “tutela da saúde, exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária”;
- g) Garantia de prevenção à fraude e à segurança do titular, nos processos de autenticação de cadastro em sistemas eletrônicos.

No que se refere à pergunta central objeto do presente estudo, qual seja, o compartilhamento de prontuários médicos entre hospitais e estabelecimentos de saúde com seguradoras de saúde são relevantes as exceções previstas nas alíneas “a”, “b” e “f”.

No Brasil, em relação ao uso primário de dados de saúde por profissionais de saúde e estabelecimentos de saúde, não há dúvidas quanto à legitimidade da coleta e armazenamento de dados de saúde em prontuários médicos, eletrônicos ou físicos, independentemente de consentimento, tendo em vista o cumprimento de obrigação legal (alínea “a”), conforme previsto no art. 69 do Código de Ética Médica, e a tutela da saúde, em procedimentos realizados junto aos pacientes (alínea “f”).

Já o uso secundário relativo ao compartilhamento de dados entre médicos e estabelecimentos de saúde com autoridades e entidades formuladoras e executoras de políticas públicas em saúde, desde que prevista em lei, apoia-se na alínea “b”, ao passo que o compartilhamento com entidades de pesquisa vem autorizado pela alínea “c”, devendo ser adotadas as providências para anonimização dos dados. Embora ambos os usos independam de consentimento do titular de dados, deve ser observada a indispensabilidade ou necessidade estrita de cada atividade específica de tratamento para atendimento da finalidade pretendida. Isso significa que a política pública que justifica o compartilhamento deve ter a finalidade de tratamento especificamente destacada em previsão legal ou regulatória, não sendo suficiente previsões genéricas de objetivos para o tratamento.

Já quanto ao compartilhamento entre hospitais e operadoras de planos de saúde tem como base legal, além do consentimento do titular, o cumprimento de obrigação legal e regulatória, alínea “a”. Trata-se do conjunto de informações a serem transmitidas conforme o padrão TISS conforme Resolução ANS 305/2012, quais sejam: (i) dados para identificação do beneficiário; (ii) dados para indicar o procedimento a ser adotado que já podem trazer indicações sobre o estado de saúde do paciente; (iii) comunicação de internação ou alta do beneficiário; (iv) dados necessários a realização das cobranças pelos serviços de saúde prestados pelos médicos e estabelecimentos de saúde envolvidos; (v) demonstrativos de retorno; (vi) trocas de documentos necessários para a autorização cobrança e glosa; (vii) dados necessários para análise de possíveis glosas.

Dentre os itens acima apenas os itens (ii) e (vii) envolvem elementos que indicam o estado de saúde do paciente. Porém, em relação ao primeiro, trata-se de uma decorrência indireta da necessidade de indicação do procedimento a ser realizado, do qual se pode inferir a condição de saúde. Já em relação ao segundo, a condução de uma auditoria para verificação da adequação do procedimento médico realizado, há informações diretas sobre o estado de saúde que podem incluir o conteúdo de prontuários e resultados de exames.

Porém, para a consecução da finalidade de uma auditoria para verificação de cobrança e glosa não é necessária a transferência de dados completos de prontuários médicos à seguradora de saúde. Como esclarecido, acima, o acesso a esses dados pode ser e usualmente é realizado durante procedimentos de auditoria, por médicos auditores e com verificação *in loco*. Assim, tendo em vista o princípio de necessidade da LGPD (art. 6º, inc. II) e o requisito de indispensabilidade da atividade de tratamento (art. 11, inc. II da LGPD) para se admitir a exceção ao consentimento, não há base outra base legítima para transferência ou compartilhamento ou concessão de acesso a dados do prontuário médico por estabelecimentos de saúde a operadoras de planos de saúde, que não o consentimento informado do paciente (art. 11, inc. I da LGPD c.c art. 8º da LGPD).

Merece análise cuidadosa a hipótese levantada na Nota Técnica nº 3/2019/GEPIN/DIRAD-DIDES/DIDES da ANS publicada em 21.11. 2019, segundo a qual o compartilhamento e tratamento de dados de saúde por OPSs independeria de consentimento, por encontrar sua base legal na alínea f, inc. II do art. 11 da LGPD:

*“Também merece destaque a dispensa de consentimento do titular no caso de tratamento de dados pessoais para tutela à saúde (artigo 7º, VIII e artigo 11º, II, “f”), desde que “exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária”.*

*A expressão “serviços de saúde” foi incluída por alteração feita pela Lei nº 13.853, de 2019, claramente contemplando gestores públicos e privados de saúde, como as operadoras de planos privados de assistência à saúde, não apenas no atendimento assistencial, mas também na gestão do cuidado.”*

A Nota Técnica da ANS entende assim que a expressão “serviços de saúde” teria sido incluída na dicção legal justamente para contemplar operadoras de planos privados de assistência à saúde. Embora a referida Nota Técnica não traga qualquer evidência histórica ou legislativa para atribuir tal “motivação” para a inclusão do termo “serviços de saúde” naquele dispositivo, reza a boa hermenêutica jurídica que “o direito objetivo não é um aglomerado caótico de preceitos; constitui uma vasta unidade, organismo regular, sistema, conjunto harmônico de normas coordenadas, em interdependência metódica, embora fixada cada uma no seu lugar próprio”.<sup>103</sup>

Essa máxima de coerência é incorporada no pressuposto hermenêutico de que o ordenamento é resultado de uma vontade idealizada e objetivada na figura de um legislador racional. A interpretação assim postula competências ao legislador que guiam a interpretação, como o postulado de consistência e coerência, segundo o qual o legislador não dita comandos contraditórios e o postulado de precisão, segundo o qual o legislador não usa termos diferentes para um mesmo fim, nem usa um mesmo termo com sentidos diferentes.<sup>104</sup>

Assim, para identificar o sentido de um termo presente no texto legal, faz-se necessário comparar o dispositivo e o termo empregado com outros dispositivos presentes no ordenamento que dele façam uso, de modo que se avalie “o Direito todo, referente ao

103 MAXIMILIANO, Carlos, *Hermenêutica e aplicação do direito*, Forense, 1997, p. 128.

104 FERRAZ JUNIOR, T.S.; MARANHÃO, J.S.A. *Função Pragmática da Justiça na hermenêutica Jurídica: lógica do ou no direito?* REVISTA DO INSTITUTO DE HERMENÊUTICA JURÍDICA, v. 1, p. 273-318, 2007.

assunto". Por outro lado, além do dever de confrontar-se o texto sujeito a exame, não só com os restantes da mesma lei ou de leis congêneres, mas também com a legislação estrangeira sobre o assunto.<sup>105</sup>

Desse modo, cabe investigar o sentido atribuído ao termo "serviços de saúde" pelo próprio ordenamento objetivo e não por uma suposição acerca da vontade do legislador concreto.

### 3.3.3 Conceito de serviço de saúde

Como já indicado acima, na legislação tributária<sup>106</sup>, os serviços de saúde têm seu objeto restrito às atividades de atendimento hospitalar, atenção ambulatorial e atividades de diagnósticos e terapêuticas.

A análise da legislação setorial, por sua vez, permite afirmar que o conceito de *serviço de saúde* é transversal, na medida em que é relevante para os sistemas público e privado, e está intrinsecamente vinculado (i) à *atividade-fim do sistema de saúde*, que é o atendimento de saúde na adoção de medidas profiláticas, diagnóstico e tratamento de enfermidade por profissionais de saúde e (ii) aos *estabelecimentos de saúde*, constituídos pela organização e gestão sócio-técnica de profissionais, instalações e equipamentos destinados a prestação de serviços saúde.

Nessa perspectiva, os serviços de saúde são constituídos pelas redes de atenção à saúde, em seus diferentes níveis de complexidade, concretamente desenvolvidas por médicos, psicólogos, dentistas, hospitais, laboratórios e clínicas para atendimento à saúde do usuário do sistema de saúde público ou privado.

De acordo com o art. 197 da Constituição Federal, as ações e serviços de saúde são de relevância pública, cabendo ao Poder Público dispor em lei sobre sua regulamentação, fiscalização e controle, devendo sua execução ser feita diretamente ou por meio de terceiros e, também, por pessoa física ou jurídica de direito privado.

Ao regulamentar a previsão constitucional, a Lei do SUS (Lei n. 8.080/1990), define o conjunto de ações e serviços de saúde voltados ao acesso universal e igualitário que integram o sistema público de saúde, os quais englobam a atenção primária, média e de alta complexidades, os serviços de urgência e emergência, a atenção hospitalar, as ações e serviços das vigilâncias epidemiológica, sanitária e ambiental e assistência farmacêutica.

Neste sentido, de acordo com a Lei, são três grandes conjuntos de ações e serviços institucionalmente reunidos sob o SUS: (i) a atenção básica, formada pelo programa de agentes comunitários de saúde, a estratégia da família e as unidades básicas e ambulatórios hospitalares; (ii) a média complexidade, formada por unidades ambulatoriais e hospitalares especializadas públicas e privadas; (iii) e as redes de alta complexidade de referência nacional em várias especialidades médicas.<sup>107</sup>

105 MAXIMILIANO, Hermenêutica e aplicação do direito, Forense, 1997, p. 131.

106 Vide Lei Federal n. 9.656/1998 (disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/L9656compilado.htm](http://www.planalto.gov.br/ccivil_03/leis/L9656compilado.htm)) e CNAE Seção Q, Divisão 86 (disponível em: <https://concla.ibge.gov.br/busca-online-cnae.html?view=divisao&tipo=cnae&versao=10&divisao=86>.)

107 Cf. OUVÉNEY, AM., NORONHA, JC. Modelos de organização e gestão da atenção à saúde:



A semântica da Lei do SUS, em toda a sua estrutura, define que os três subsistemas correspondem a configurações específicas de *estruturas de oferta* de saúde, proporcionadas por prestadores de serviços de saúde públicos e privados desde a atenção domiciliar até hospitais especializados e de alta complexidade<sup>108</sup>.

No mesmo sentido, ao regulamentar a Lei do SUS, o Decreto n. 7.508/2011 que define que “o acesso universal, igualitário e ordenado às ações e serviços de saúde se inicia pelas portas de entrada do SUS e se completa na rede regionalizada e hierarquizada”, denotando serviços de saúde novamente como a prestação da atuação médico-hospitalar, e cria a Relação Nacional de Ações e Serviços de Saúde – RENASES, listagem que compreende todas as ações e serviços que o SUS concretamente oferece ao usuário para atendimento da integralidade da assistência à saúde, por meio dos entes federados, de forma direta ou indireta<sup>109</sup>.

Os serviços públicos de saúde também são tratados na Lei Complementar n. 141, de 14 de janeiro de 2012, que dispõe sobre o orçamento destinado à saúde pelos entes federativos em ações e serviços públicos de saúde. Nos termos da Lei Complementar, são consideradas ações e serviços públicos de saúde, para fins de apuração da aplicação dos recursos mínimos, aquelas voltadas para a promoção, proteção e recuperação da saúde, financiadas com recursos movimentados por meio dos respectivos fundos de saúde, disponíveis a população de forma gratuita e que observam as regras de governança expressas na Lei.

Portanto, ao dispor sobre serviços de saúde, a legislação setorial do SUS delimita as dimensões e a abrangência da rede de atenção à saúde que será ofertada pelo sistema público, definindo, a partir dos eixos de atendimento, qual será o arranjo de prestadores dos serviços – em um misto de oferta pública e privada –, os pressupostos mínimos de governança e as fontes de financiamento. Para que prestação dos serviços de saúde sejam adequadamente geridos pelo SUS, a atuação complementar dos prestadores privados de saúde privados toma por base as informações constantes em três bancos de Sistemas de Informação de Saúde (SIS) disponíveis no Ministério da Saúde: o Sistema de Informações

---

redes locais, regionais e nacionais. In; FUNDAÇÃO OSWALDO CRUZ. A saúde no Brasil em 2030 - prospecção estratégica do sistema de saúde brasileiro: organização e gestão do sistema de saúde [online]. Rio de Janeiro: Fiocruz/Ipea/Ministério da Saúde/Secretaria de Assuntos Estratégicos da Presidência da República, 2013. Vol. 3. pp. 143-182.

108 Serviços de saúde como redes de atendimento: HARTZ, Z. M. A.; CONTANDRIOPOULOS, A. P. Integralidade da atenção e integração de serviços de saúde: desafios para avaliar a implantação de um “sistema sem muros”. Cadernos de Saúde Pública, Rio de Janeiro, v. 20, supl. 2, p. S331-S336, 2004. MATOS, C. A.; POMPEU, J. C. Onde estão os contratos? Análise da relação entre os prestadores privados de serviços de saúde e o SUS. Ciência & Saúde Coletiva, Rio de Janeiro, v. 8, n. 2, p. 629-643, 2003. MENDES, E. V. Sistemas integrados de serviços de saúde: a reforma microeconômica dos sistemas de serviços de saúde. Mimeo., 2000. ZUCCH, I. P.; NERO, C. D.; MALIK, A. M. Gastos em saúde: os fatores que agem na demanda e na oferta dos serviços de saúde. Saúde e Sociedade, São Paulo, v. 9, n. 1/2, p. 127-150, 2000. SANTOS, M. A. B. Terceirização da prestação de serviços de saúde no SUS: o caso das análises clínicas. 2012. 144f. Tese (Doutorado em Ciências na área de Saúde Pública.) – Escola Nacional de Saúde Pública, Fiocruz, Rio de Janeiro. Santos, Maria Angélica dos Contratualização e remuneração de serviços de saúde no SUS: situação atual e perspectivas / Maria Angélica Borges dos Santos, Luciana Mendes Santos Servo. – Rio de Janeiro: Fundação Oswaldo Cruz, 2021.

109 Portaria n. 841, de 2 de maio de 2012. Publica a Relação Nacional de Ações e Serviços de Saúde (RENASES) no âmbito do Sistema Único de Saúde (SUS) e dá outras providências.

Hospitais (SIH)<sup>110</sup>, o Sistema de Informações Ambulatoriais (SIA)<sup>111</sup> e o Cadastro Nacional de Estabelecimentos de Saúde (CNES)<sup>112</sup>.

No âmbito da saúde complementar a menção a serviços de saúde permanece com a mesma semântica da legislação do SUS.

Na Lei dos Planos de Saúde (Lei n. 9.656/1998), serviços de saúde são equiparados, em diferentes dispositivos, aos estabelecimentos de saúde e aos serviços de saúde em si. Ao conceituar plano privado de assistência à saúde, a Lei estipula que a assistência à saúde do beneficiário dar-se-á pela faculdade de acesso e atendimento por profissionais ou *serviços de saúde*, livremente escolhidos, integrantes ou não de rede credenciada, contratada ou referenciada. Ou seja, neste dispositivo, estabelecimentos de saúde e serviços de saúde são tratados como sinônimos.<sup>113</sup> Em outro dispositivo, ao tratar dos requisitos que a OPS deverá observar para obter a autorização de funcionamento, a Lei estabelece que a operadora deverá descrever, de maneira pormenorizada, os *serviços de saúde* próprios oferecidos e daqueles a serem prestados *por terceiros*, adotando aqui serviços de saúde em sua conotação de atividade finalística da saúde, com a prestação do serviço em si mesmo (art. 8º, inciso II)<sup>114</sup>, que será remunerado pela operadora de saúde, mas prestado por terceiros, i.e, médicos, profissionais de saúde e estabelecimentos de saúde. Ainda neste sentido, ao tratar da formalização de contratos, a Lei prevê que a prestação de *serviços de assistência à saúde* no âmbito dos planos privados de assistência à saúde será realizada por pessoas físicas (profissionais de saúde em prática liberal privada) ou jurídicas (estabelecimentos de saúde), independentemente de sua qualificação como contratadas, referenciadas ou credenciadas (art. 17-A).

Por sua vez, a Lei n. 9.961/2000, ao dispor sobre as competências da ANS, atribui à Agência poderes para “estabelecer normas relativas à adoção e utilização, pelas operado-

---

110 O SIH/SUS, tem origem nas *Autorizações de Internação Hospitalar* (AIH), destinadas ao pagamento das internações de hospitais públicos e privados conveniados ao SUS.

111 O SIA/SUS engloba todos os procedimentos de assistência à saúde que não exijam internação, sendo amplamente descentralizado nos Estados e municípios, além de refletir a produção mensal das unidades do SUS. Neste sistema, também estão disponíveis as Fichas de Programação Físico-Orçamentária (FPO) e as Fichas de Cadastro das Unidades (FCA) que, mesmo não sendo atualizadas com a periodicidade necessária, permitem a caracterização das unidades e dos gestores.

112 Cadastro Nacional de Estabelecimentos de Saúde (CNES) - Portaria nº 1.646, de 2 de outubro de 2015

Art. 5º O CNES é a fonte de informações oficial sobre estabelecimentos de saúde no país, devendo ser adotado por todo e qualquer sistema de informação que utilize dados de seu escopo e ser utilizado como fonte para todas as políticas nacionais de saúde.

113 Lei n. 9.656/1998

Art. 1º, I - Plano Privado de Assistência à Saúde: prestação continuada de serviços ou cobertura de custos assistenciais a preço pré ou pós estabelecido, por prazo indeterminado, com a finalidade de garantir, sem limite financeiro, a assistência à saúde, pela faculdade de acesso e atendimento por profissionais ou serviços de saúde, livremente escolhidos, integrantes ou não de rede credenciada, contratada ou referenciada, visando a assistência médica, hospitalar e odontológica, a ser paga integral ou parcialmente às expensas da operadora contratada, mediante reembolso ou pagamento direto ao prestador, por conta e ordem do consumidor; ([Incluído pela Medida Provisória nº 2.177-44, de 2001](#))

114 Lei n. 9.656/1998

Art. 8º para obter a autorização de funcionamento, as operadoras de planos privados de assistência à saúde devem satisfazer os seguintes requisitos, independentemente de outros que venham a ser determinados pela ANS: (...) II - descrição pormenorizada dos serviços de saúde próprios oferecidos e daqueles a serem prestados por terceiros;

ras de planos de assistência à saúde, de mecanismos de regulação do uso dos *serviços de saúde* (art. 4º, inciso VII) e para “fiscalizar a atuação das operadoras e *prestadores de serviços de saúde* com relação à abrangência das coberturas de patologias e procedimentos” (art. 4º, inciso XXVI)”. Portanto, no âmbito desta Lei, há uma clara distinção entre “prestadores de serviços de saúde” e “operadoras de saúde”, sendo o termo *serviço de saúde* à prestação concreta da assistência diagnóstica ou terapêutica à saúde do beneficiário.

Nesses termos, a legislação setorial aponta para um conceito estrito de *serviços de saúde*, que se limita a definir os *serviços de saúde* como o atendimento pelo profissional de saúde (médicos e enfermeiros) e estabelecimentos de saúde (hospitais, clínicas e ambulatórios) aos *pacientes* com a finalidade profilática diagnóstica ou terapêutica.

Não há na legislação uma correspondência entre “*serviços de saúde*” com “*todos os elos da cadeia de saúde complementar*” de forma global, de modo que incluir as operadoras de planos de saúde na extensão semântica do termo “*serviços de saúde*” presente no art. 11, II, “f” da LGPD, seria atribuir significativa imprecisão e incoerência ao ordenamento, por estipular sentido e alcance muito mais abrangente a “*serviços de saúde*” do que aquele previsto na legislação setorial. E isso justamente na interpretação de uma exceção à exigência de consentimento para garantia da autonomia informativa do paciente. A exceção, como reza a boa hermenêutica, interpreta-se restritivamente e não de modo ampliativo.

Parece mais harmônico diante da legislação setorial entender que a alteração introduzida pela Lei 13.853/2019, ao incluir o termo “*serviços de saúde*” ao lado de “*profissionais de saúde*” e “*entidades sanitárias*” tenha objetivado não limitar o tratamento de dados de saúde, no contexto de atendimento ao paciente, aos profissionais de saúde, pessoas físicas, mas se referir também aos *estabelecimentos de saúde*, tendo em vista a complexa estrutura de prestação do *serviço de saúde*, que não se restringe aos profissionais, mas abrange todas as instalações, equipamentos e análise de informações por aqueles envolvidos em “*procedimento médico*”.

Essa leitura não só é a mais coerente observando-se a legislação setorial, como também se observando a sistemática da própria LGPD. Com efeito, a própria alínea “f” fala da autorização do tratamento de dados “*exclusivamente, em procedimento médico*”, o que indica o contexto específico de atenção, típico daquilo que os europeus chamam de “*uso primário*” dos dados de saúde. A interpretação ampliativa, para incorporar usos secundários e em particular o uso por uma operadora de saúde, para gestão de pagamentos, não conversa com dois fatos. Em primeiro lugar, os demais usos secundários para ações relativas à saúde estão previstas em exceções próprias, como o cumprimento a obrigação legal, execução de políticas públicas ou uso para finalidade de pesquisa científica, não havendo razão para incorporar sub-repticiamente seguradoras de saúde em alínea que trata especificamente de procedimentos médicos. Em segundo lugar, porque a própria LGPD traz uma preocupação em relação à exploração de dados de saúde para outras finalidades que não a tutela da saúde, como a obtenção de vantagem econômica e, especificamente, para operadoras de saúde, prevê, no seu parágrafo 5º ser “*vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários*”.

Como a atividade precípua das operadoras de saúde é a intermediação financeira da prestação de *serviços de saúde* por médicos e estabelecimentos de saúde, não faria senti-

do, considerando o princípio de necessidade da LGPD, admitir que dados de prontuários médicos poderiam ser compartilhados com seguradoras de saúde para um uso secundário. Entender que as seguradoras poderiam armazenar os dados, mas não os utilizar para outros fins, também seria descabido, pois o armazenamento é também uma forma de tratamento de dados, que precisa de base legal própria além de satisfazer do requisito de indispensabilidade, que parece não estar presente aqui.

Quanto à possível alegação de que operadoras de saúde desenvolvem programas de gestão de cuidado, com ações de prevenção a doenças, há duas hipóteses.

A primeira seria a de que tal gestão de cuidado configuraria a prestação de um serviço médico. Nesse caso, seu exercício, conforme legislação setorial, somente pode ser realizado por médicos e profissionais de saúde, em procedimentos conduzidos em estabelecimentos de saúde. São estes profissionais e entidades que consultarão e manterão os registros médicos nos respectivos prontuários. Portanto, nesta hipótese, nada se altera em relação à seguradora, que continua no papel de intermediador financeiro da relação entre pacientes, de um lado, e médicos e estabelecimentos, de outro.

A segunda hipótese seria a de que a seguradora faria a gestão de informações e dados presente em prontuários médicos e outros aplicativos de saúde para prover os pacientes de informações e sobre saúde e bem estar para promover hábitos saudáveis pelos pacientes. Nesse caso, não há serviço médico prestado, apenas informações sobre saúde, caso no qual a posição das seguradoras não difere de outros aplicativos disponíveis no mercado para orientação e apoio aos indivíduos sobre hábitos de saúde, como, por exemplo, aplicativos que fazem mensuração e informam um indivíduo diabético sobre seu grau de glicose para que este então administra dosagens de insulina. Tais aplicativos dependem integralmente do consentimento do titular de dados para o acesso a esses dados de saúde.

### **3.3.4 Direito comparado e a Regulamentação do Programa Conecte SUS**

Como visto na análise da experiência internacional, em particular da legislação europeia na qual se baseia a legislação nacional, há uma distinção fundamental entre o *uso primário dos dados de saúde*, que se restringe ao tratamento de dados no contexto específico de atendimento ao paciente por profissionais de saúde ou de assistência social e *usos secundários* consistentes na utilização para formulação de políticas de saúde e gestão do sistema de saúde, além do uso para finalidade de pesquisa. Também na GDPR há uma exceção ao consentimento de tratamento de dados sensíveis por profissionais de saúde, conforme legislação específica de cada Estado-Membro ou por força de contrato com o profissional de saúde. O direcionamento aqui para a exceção relaciona-se, assim ao atendimento pelo profissional de saúde, no estabelecimento de saúde no ponto específico de cuidado e atenção ao paciente.

Também se nota essa diferença de tratamento nos sistemas inglês, norte-americano e argentino, em que há autorização para acesso e utilização de dados de prontuários médicos pelos profissionais de saúde e estabelecimentos de saúde no contexto de prevenção, diagnóstico ou tratamento de pacientes, ao passo em que outros usos, para a finalidade de pesquisa, gestão de pagamento ou políticas públicas, dependem fundamentalmente

do consentimento do titular de dados (com exceção do sistema inglês, que, como visto, adota um modelo de *opt out* para usos secundários).

Não há motivos para se interpretar que a legislação nacional de proteção de dados, com a introdução da alínea “f”, no inc. II do art. 11 da LGPD tivesse por objetivo destoar e divergir da experiência internacional, que restringe o acesso aos prontuários eletrônicos aos médicos e estabelecimentos de saúde nos pontos de atenção, para abrir esses dados a intermediadores financeiros ou à fonte pagadora do sistema de saúde. Como analisado acima, tudo indica que, a LGPD, ao enfatizar que a exceção ao consentimento se dá exclusivamente “*em procedimento médico*”, fez referência ao uso primário dos dados para o contexto específico de atendimento médico, diagnóstico, preventivo ou terapêutico.

Aliás, essa também foi a solução adotada pela Portaria 1434/2020 que institui o programa Conecte SUS e a iniciativa de criação de uma Rede Nacional de Dados em Saúde-RNDS, que é baseado nas seguintes premissas:

- i) Os dados de saúde são compartilhados apenas com os profissionais de saúde ligados ao SUS;
- ii) O profissional de saúde somente pode acessar os dados de um indivíduo durante um contato assistencial;
- iii) O indivíduo poderá ativamente exercer o direito de se retirar do processo de compartilhamento de dados pessoais de saúde da RNDS e gerir o acesso por profissionais de saúde conforme seu consentimento expresso;
- iv) O indivíduo titular de dados pessoais tem o direito de ser informado sobre a finalidade de tratamento de seus dados.

Se esse é o regime em relação aos dados de atendimentos gerados pelo SUS, com o estrito acesso por profissionais de saúde, em contatos assistenciais, não parece acurado entender que o sistema na rede privada deveria ser diferente, com a possibilidade de acesso por terceiros, como seguradoras de saúde, aos dados médicos do paciente. Como destaca Oliveira et.al., “*o acesso aos dados da RNDS está restrito ao titular, mediante autenticação realizada por meio de acesso GOV.BR; e aos profissionais de saúde, mediante autenticação da Certificação Digital ICP-Brasil de instalações de Prontuário Eletrônico do Paciente previamente habilitada para o estabelecimento de saúde e quando respeitado o contexto de atendimento, isto é, apenas quando o profissional de saúde está atuando diretamente no procedimento de saúde do cidadão do qual pretende obter a história clínica disponível*”. O mesmo regime deve prevalecer em relação aos médicos e estabelecimentos privados de saúde.

### **3.4.5 Considerações sobre a implantação de interoperabilidade e o acesso a prontuários eletrônicos no Brasil**

Conforme levantado neste estudo, a digitalização de prontuários médicos e sua interoperabilidade são consideradas, em diferentes países, como fundamental para o aumento de eficiência e segurança dos serviços de saúde bem como para a consolidação de uma medicina centrada no paciente com a solução de continuidade no tratamento e promoção de seu bem-estar.

Na experiência internacional, o vetor de implantação da interoperabilidade está no foco de atenção e cuidado, ou seja, no contexto específico de atendimento por profissionais de saúde em estabelecimentos de saúde, de forma presencial ou remota. Essa solução tem duas vantagens: (i) em primeiro lugar, faz com que os incentivos e objetivos de eficiência decorrentes da interoperabilidade estejam não na redução de custos, mas fundamentalmente no bem estar do paciente, promovido pelos profissionais de saúde (muito embora a redução de custos, com a solução de continuidade no tratamento, seja uma decorrência natural da interoperabilidade); (ii) em segundo lugar, assegura a privacidade e proteção de dados, por restringir o acesso aos dados aqueles profissionais e agentes estritamente necessários para a condução do tratamento médico.

Em um sistema centrado no paciente, porém, o vetor de interoperabilidade deve estar no ponto de atenção e cuidado e não da perspectiva de redução de custos, sob pena de criação de incentivos para discriminações. Ou seja, a interoperabilidade deve ser focada naqueles que provém o cuidado, que mantém a relação com os usuários na condição de pacientes, e não na fonte pagadora do sistema de saúde.

Essa mesma orientação está presente nos normativos e programas de inovação nacionais no setor de medicina. Assim, a Estratégia de Saúde Digital para o Brasil 2020-2028 traz a digitalização e interoperabilidade como pilares do desenvolvimento nacional, mas refere a interoperabilidade a uma integração entre estabelecimentos de saúde e profissionais de saúde apenas. Também a regulamentação da Rede Nacional de Dados de Saúde restringe o acesso a dados de saúde ao estabelecimento de saúde e profissionais de saúde diretamente envolvidos no contexto de atendimento ao paciente. Além disso, a Lei Geral de Proteção de Dados assenta-se no princípio de necessidade e finalidade no tratamento de dados, incluindo os dados de saúde dentre os dados sensíveis, o que, por si, exclui operadoras de saúde do acesso a prontuários médicos ou seu compartilhamento. Ademais, como visto, a autorização de tratamento de dados de saúde, em procedimento médico, por profissionais de saúde e *serviços de saúde* refere-se, em consonância com o conceito de serviços de saúde presente em nosso ordenamento, a médicos e estabelecimentos de saúde. Por fim, a legislação setorial estabelece de modo detalhado as informações a serem compartilhadas entre estabelecimentos de saúde e seguradoras de saúde, conforme o padrão TISS. Ou seja, não há base legal para compartilhamento de dados de saúde com operadoras de saúde.

Como vimos também, empresas de seguro saúde, mesmo com programas de estímulo a prevenção, continuam sendo intermediadores financeiros e fontes de custeio aos profissionais e estabelecimentos que prestam atendimento à saúde. Se prestam serviços de saúde, então os fazem necessariamente por meio de médicos e estabelecimentos de saúde. Se prestam serviços de orientação e informação sobre hábitos saudáveis e boas práticas de saúde, então necessitam do consentimento de seus beneficiários para acessar dados sensíveis sobre sua condição de saúde.

Aparentemente, porém, um conjunto de iniciativas tem indicado caminho diverso da tendência e das melhores práticas internacionais, com a proposição de que as seguradoras de saúde deveriam ser os vetores da interoperabilidade. Assim, por exemplo, a exigência por seguradoras de saúde de compartilhamento de prontuários médicos no momento de cadastramento dos estabelecimentos de saúde ao plano. Ou ainda, o Projeto de Lei 3815/2020,

que propõe a criação de um prontuário eletrônico único e centralizado no Estado, reunindo informações não só dos hospitais públicos como também dos estabelecimentos de saúde privados. Por fim, a indicação de uma portabilidade e compartilhamento de informações entre Operadoras de Planos de Saúde, em manifestações do Exmo. Ministro da Saúde em veículos de comunicação, como base de um programa de *Open Health*.

O compartilhamento de prontuários médicos entre OPSs traz as seguintes desvantagens e riscos:

- a) *Distorção dos incentivos*: desloca a interoperabilidade para a fonte pagadora, o que concentra os incentivos na redução de custos e não na saúde do paciente;
- b) *Problema de inclusão*: considerando que apenas parte da população é atendida pela saúde suplementar, a implementação da interoperabilidade pelas OPSs significa que parte da população não obterá os benefícios de eficiência e continuidade do tratamento, gerando um problema de inclusão social;
- c) *Conflitos entre standards técnicos*: diferentes OPSs, como empresas privadas, podem utilizar padrões técnicos e terminologias distintas entre si, o que significaria uma interoperabilidade fragmentada, vigente apenas entre cada OPS. Isso contraria a experiência internacional, em que uma política pública nacional estipula padrões uniformes a serem atendidos pelos estabelecimentos de saúde, de modo que todos os sistemas estejam integrados;
- d) *Distorções concorrenciais*: como OPSs no Brasil estão verticalmente integradas a hospitais, isso significa que a interoperabilidade via seguradoras de saúde traria uma assimetria entre hospitais integrados a OPSs, que teriam informações sensíveis sobre seus concorrentes, e hospitais não integrados, sem acesso a informações concorrencialmente relevantes, o que, como visto na próxima seção, pode trazer prejuízos à concorrência, considerando a elevada concentração no setor.

Portanto, além de não estar albergada pelo ordenamento nacional, a adoção de uma política para introduzir a interoperabilidade pelas seguradoras de saúde seria contraproducente e contrária as melhores práticas internacionais.

Em relação à adoção de prontuário único, como vimos, a introdução de um modelo de saúde digital e de interoperabilidade entre prontuários eletrônicos pode ser obtida por meio do que chamamos de interoperabilidade de dados, em que a chave está no acesso *mútuo* pelos profissionais de saúde e estabelecimentos de saúde a diferentes plataformas que sigam os mesmos padrões técnicos e semânticos, não havendo necessidade de transferência e concentração dos dados em uma única plataforma.

A concentração de dados sob o controle do Estado traz à tona o que Spiros Simitis denominou de “ameaça da unidade informacional”, que contraria a chamada separação de poderes informacional, corolário do direito fundamental à proteção de dados.

Spiros Simitis, considerado o fundador da disciplina de proteção de dados, em sua análise do famoso caso do censo alemão, no qual a corte constitucional alemã reconheceu, pela primeira vez, o direito à autodeterminação informacional, nota que a corte alemã naquela oportunidade estabeleceu uma nova divisão de poderes dentro do Estado, a divisão de poderes informacional, na medida em que postulava ser

incompatível com a proteção de dados a possibilidade de administração pública e o Estado serem concebidos como uma *unidade informacional*.<sup>115</sup>

Para se atingir tal objetivo, impedindo a cristalização da unidade informacional como poder fático, atrela-se o princípio da finalidade à estrita definição de competências de cada órgão público.<sup>116</sup> Do ponto de vista da divisão constitucional de competências, somente se justifica o tratamento de dados por uma unidade da administração pública, na medida em que este se insira no âmbito das atribuições específicas dos órgãos ou entidades que exerçam funções públicas.<sup>117</sup> A competência determina previamente a finalidade claramente identificável, a qual restringe não apenas as transferências para particulares, ou a transferência de dados de particulares para o Estado, como também a transferência de dados pessoais no próprio seio da Administração Pública.<sup>118</sup>

Além da ameaça da unidade informacional nas mãos do Estado, que não se justifica sob o prisma de necessidade, uma vez que os objetivos podem ser alcançados com a interoperabilidade no acesso padronizado aos dados descentralizados por estabelecimentos e profissionais de saúde, há também o maior risco de segurança, tendo em vista que uma violação a uma central que armazena todo o histórico de saúde de todos os cidadãos do País poderia ter impactos gravíssimos sobre a sociedade, valendo lembrar o recente incidente de segurança envolvendo o ConectSUS.<sup>119</sup>

Por fim, em relação ao programa de *Open Health*, embora não haja ainda uma divulgação oficial dos termos dessa nova política para o setor de saúde,<sup>120</sup> levanta-se a preocupação quanto à previsão de “portabilidade” ou de trocas de dados de saúde entre operadoras de planos de saúde. Com base na experiência internacional aqui analisada, os objetivos de aumento de eficiência e continuidade no tratamento, em uma medicina centrada no paciente, são alcançados pela interoperabilidade nos pontos de atenção e não na troca de dados pessoais entre as fontes pagadoras.

Se a noção de *Open Health* no programa anunciado na imprensa estiver baseada na troca direta de informações entre seguradoras de saúde, independentemente de consentimento dos titulares, então eventual legislação que introduza tal permissão certamente será questionável frente ao direito fundamental constitucional de proteção aos dados pessoais, cf. LXXIX do art. 5º da CF88 (introduzido pela EC 115/2022). O *Open Health* somente seria admissível, em termos de portabilidade dos dados por manifestação de vontade do titular dos dados. Ou seja, em se tratando da transferên-

---

115 Spiros Simitis: *Die informationelle Selbstbestimmung - Grundbedingung einer verfassungskonformen Informationsordnung* (NJW 1984, 398), p. 403.

116 Na tradição europeia, o princípio da finalidade não é absoluto. Os dados pessoais recolhidos uma vez para determinados fins podem, sob certas condições, ser (posteriormente) processados para outros fins. O critério decisivo é a compatibilidade. A finalidade original e a nova finalidade não devem ser incompatíveis. Para tanto ver Manfred Monreal: *Weiterverarbeitung nach einer Zweckänderung in der DS-GVO*, In: Zeitschrift für Datenschutz 2016, p. 507ss.

117 Spiros Simitis. *Von der Amtshilfe zur Informationshilfe - Informationsaustausch und Datenschutzanforderungen in der öffentlichen Verwaltung*, In: Neue Juristische Wochenschrift 1986, 2795

118 Hans Peter Bull. *Datenschutz contra Amtshilfe*. In: Die Öffentliche Verwaltung 1979, p. 689-696.

119 <https://g1.globo.com/saude/noticia/2021/12/10/pf-e-gabinete-de-seguranca-institucional-vao-investigar-incidente-no-conectesus-diz-ministerio-da-saude.ghtml>

120 <https://www1.folha.uol.com.br/opinioao/2022/03/por-que-o-open-health.shtml>



cia dos dados do beneficiário titular, mediante solicitação do próprio usuário e apenas aquelas informações detidas pela seguradora de saúde (que, por tudo o que foi analisado até aqui, somente incluiria dados de prontuários médicos mediante consentimento explícito e informado do titular do dado).

## 4. Potenciais problemas concorrenciais derivados do compartilhamento de dados sensíveis de saúde às operadoras de planos de saúde

O compartilhamento e a interoperabilidade de dados têm sido apontados como uma das alternativas para enfrentar, na economia digital, o problema da concentração de dados, pessoais ou não, em poucas plataformas dominantes. Como os dados e sua análise são ativos essenciais na economia digitalizada para o aumento de eficiência dos serviços e as empresas dominantes possuem uma posição privilegiada no acesso e tratamento desses dados, cria-se uma barreira a entrada a novos agentes que pretendam participar de determinado mercado.

Uma política de compartilhamento, porém, a não ser na hipótese do abuso de poder econômico por determinado agente em que o compartilhamento pode ser determinado pela autoridade antitruste, deve ser adotada de modo uniforme, sob pena de criar distorções. Uma possível distorção estaria no compartilhamento de dados entre hospitais privados e operadoras de planos de saúde, tendo em vista que parte das operadoras são verticalmente integradas a hospitais concorrentes.

Desse modo uma interoperabilidade estruturada nas Operadoras de Planos de Saúde, poderia beneficiar hospitais controlados por essas operadoras, que poderiam ter acesso a informações de seus concorrentes, sem que o mesmo ocorra para hospitais não integrados.

Atento aos novos modelos de negócios, cada vez mais centrados em tecnologias de armazenamento e processamento de dados, o Conselho Administrativo de Defesa Econômica – CADE tem ressaltado em suas análises a relevância dos dados para o processo competitivo e o seu acesso na condição de vantagem competitiva<sup>121</sup>.

Essa preocupação, que se reflete na análise de atos de concentração e na apuração de ilícitos antitruste, se torna especialmente relevante em mercados concentrados, nos quais grupos econômicos com poder de mercado podem se valer de sua dominância para obter informações de agentes econômicos com menor poder de barganha em mercados à jusante ou relacionados, sem que haja justificativa legal adequada para esse compartilhamento. Essas características podem ser observadas na cadeia de saúde suplementar no Brasil.

O mercado de saúde suplementar é marcado por um processo de concentração, com o crescimento e consolidação de grupos econômicos que se tornaram líderes em seus mercados de atuação. Esse movimento está ligado à entrada de capital externo no mercado de saúde suplementar<sup>122</sup>, quer permitiu a utilização de fusões e aquisições como estratégias de crescimento, havendo uma expansão desses grupos ao longo da cadeia produtiva, seja para mercados verticalmente relacionados, seja para mercados complementares, ampliando o portfólio desses grupos.

Especificamente, operadoras de planos de saúde tem buscado ao máximo possível expandir sua carteira de beneficiários para diluição de riscos devido a assimetria de informação com prestadores de serviço e com consumidores. As normas regulatórias impõem determinados requisitos econômico-financeiros mínimos que induzem o ganho de escala, além dos custos existentes no investimento em marca que exigem a operação por um período longo no mercado para serem recuperados. Por sua vez, há custos crescentes advindos inovações tecnológicas.

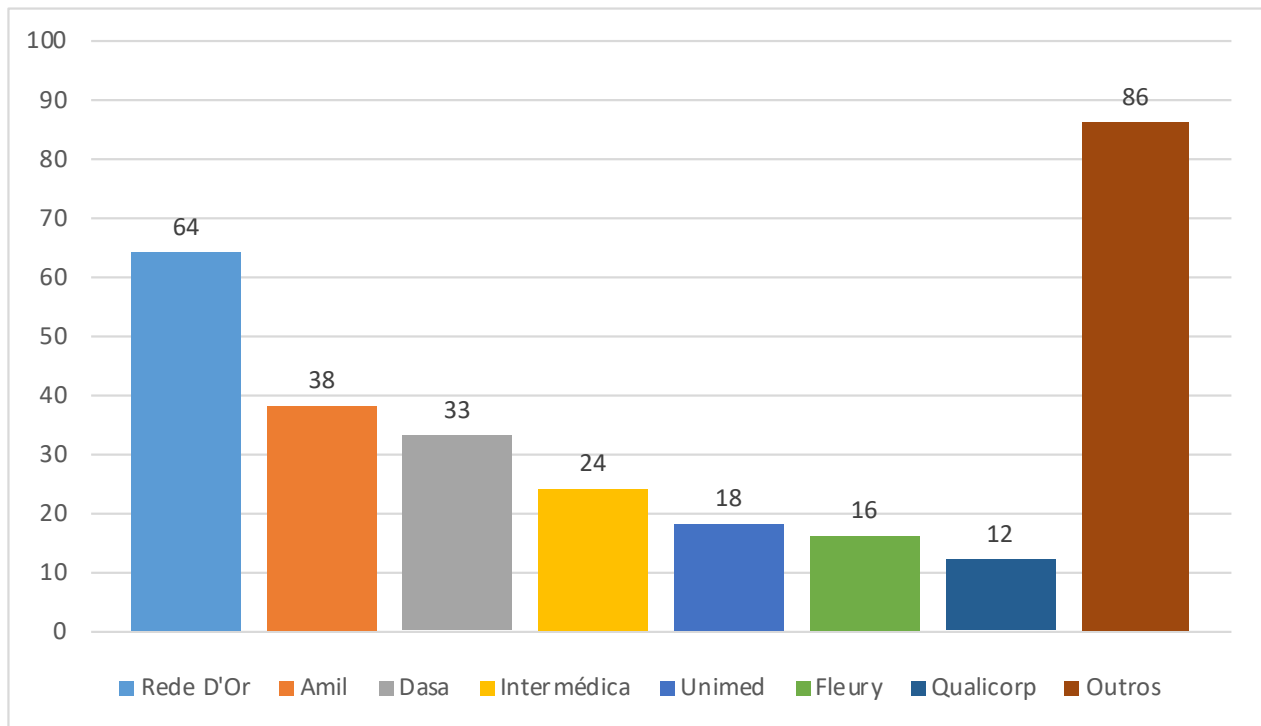
Tais características induzem à concentração horizontal entre operadoras de saúde, bem como à verticalização com prestadores de serviços no mercado à jusante, em especial hospitais e agentes de medicina diagnóstica. Isso pode ser observado principalmente a partir dos atos de concentração por grupo econômico no setor nos últimos anos. Note-se que Rede D'Or, Amil, Dasa, Notre Dame Intermédica, Fleury, Unimed e Qualicorp respondem por 72,43% dos casos analisados pelo CADE entre 2003 e 2021:

---

121 Cf. Ato de Concentração nº 08700.003969/2020-17, entre STNE Participações S.A. e Linx S.A.; Ato de Concentração nº 08700.006373/2020-61, entre Claro S.A. e Serasa S.A.; e Ato de Concentração nº 08700.000059/2021-55, entre Magalu Pagamentos Ltda. e Hub Prepaid Participações S.A.

122 A partir de 2000, houve a liberação da participação de capital estrangeiro nos mercados de saúde suplementar no Brasil. Essa permissão foi inserida com a Lei nº 9.656/1998, ao permitir a participação de pessoas físicas ou jurídicas domiciliadas no exterior participarem do capital de pessoas jurídicas nacionais voltadas a operar planos privados de assistência à saúde. Por sua vez, a Lei nº 13.097/2015 estendeu essa possibilidade também para empresas de assistência à saúde.

## Atos de concentração por grupo econômico (2003 - 2021)



Fonte: DEE/CADE<sup>123</sup>

Esse cenário de alta concentração horizontal somada à verticalização e a presença de elevadas barreiras à entrada tornam o ambiente concorrencial preocupante por favorecer o exercício de poder de mercado por parte das OPS à montante e à jusante na cadeia. Certas práticas podem chamar a atenção da autoridade concorrencial principalmente quando exercidas com relação a *players* não verticalizados no mercado à jusante ou com baixo poder de barganha, fator que é relevante no contexto do mercado de saúde complementar<sup>124</sup>.

De fato, a jurisprudência do CADE<sup>125</sup> reconhece de maneira ampla que os prestadores de serviços de saúde se encontram em situação assimétrica com relação às OPSs,

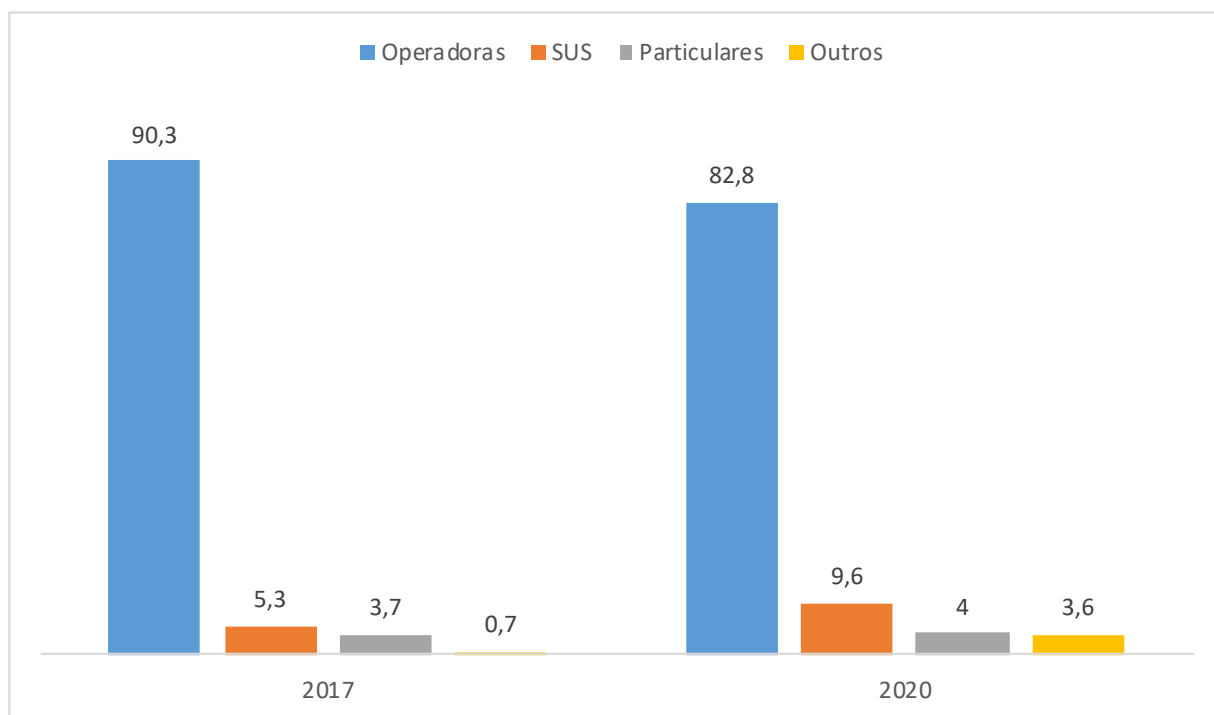
123 Departamento de estudos Econômicos (DEE) – CADE. Cadernos do Cade - Mercado de Saúde Suplementar: Condutas (Edição revista e atualizada). Brasília, 2022. Disponível em: [https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/estudos-economicos/cadernos-do-cade/Caderno-Saude-Suplementar\\_Condutas\\_Atualizado-VFinal.pdf](https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/estudos-economicos/cadernos-do-cade/Caderno-Saude-Suplementar_Condutas_Atualizado-VFinal.pdf)

124 Vale notar que as práticas anticoncorrenciais mais comuns investigadas pelo CADE nesse mercado possuem como raiz justamente a relação entre os prestadores de serviço médico e planos de saúde, justamente por conta dessa assimetria que muitas vezes tenta ser compensada por meios não admitidos pela autoridade.

125 Essa posição pode ser destacada no Processo Administrativo nº 08012.006923/2002-18, onde o então Conselheiro Marcos Paulo Veríssimo destacou que a assimetria de poder entre os agentes verticais da cadeia deveria ser um elemento trazido na análise de condutas anticompetitivas no setor, principalmente quando se aventaria a possibilidade de aplicar a teoria do poder compensatório. Isso é reforçado no Processo Administrativo n. 08012.006552/2005-17 em que a Conselheira Ana Frazão destaca a situação fática claramente desigual entre as OPS e prestadores de serviços médicos. Essa assimetria é mais intensa quando se considera os prestadores individualmente enquanto médicos, mas pode ser sentida também em fatores como clientela e fonte de receita no que diz respeito aos hospitais, laboratórios e clínicas.

sobretudo as operadoras verticalizadas. Isso se deve à relação de dependência criada entre esses agentes, na medida em que a maior parte de suas receitas têm as operadoras como fonte pagadora. Nesse sentido, em 2020, mais de 80% da receita obtida por hospitais privados originou-se justamente dessa fonte, enquanto os pagamentos diretos dos particulares e do SUS atingem taxas muito baixas:

## Fontes de Recursos de Hospitais Privados



Fonte: Observatório da ANAHP/2021

Como visto, para a consecução das atividades das OPAs, que consiste basicamente na intermediação facilitada entre os beneficiários e os prestadores de serviços de saúde (médicos, hospitais, clínicas e laboratórios), exige-se o compartilhamento de um número reduzido de informações e dados pessoais, de modo que o compartilhamento integral do prontuário eletrônico dos pacientes beneficiários não possui uma base legal adequada para tanto. Nesse contexto, a exigência de compartilhamento excessivo de dados pessoais por parte dos prestadores de serviços médicos a OPS pode ter implicações concorrenciais sensíveis.

Em primeiro lugar, a própria exigência é problemática. A utilização da assimetria de poder existente entre o agente em posição dominante no mercado à montante em face do agente no mercado à jusante para obtenção de dados sem adequada base legal impõe ao concedente a escolha entre infringir a legislação de proteção de dados ou ser retaliado, tendo em vista a relação de dependência.

Ademais, essa conduta pode revelar, na verdade, o desenvolvimento de práticas anticompetitivas que se inserem no modelo de negócios das operadoras de saúde em um cenário de concentração econômica, em mercados relacionados ou próximos.

Operadoras de planos de saúde baseiam sua atuação com base na gestão de riscos e expectativas de receitas e despesas. A obtenção de informações dos beneficiários a partir de prontuários eletrônicos compartilhados, *a princípio*, pode não representar qualquer vantagem competitiva, mas quando obtidas em grande volume podem representar subsídio para o desenvolvimento indevido de modelos atuariais mais eficientes, de modo que quanto maior o número de informações obtidas maior será a vantagem, o que claramente tende a favorecer os grandes *players* do mercado com os maiores números de beneficiários. Desse modo, o desenho de soluções mais eficientes a partir desses dados tende a favorecer a alavancagem das operadoras já em posição dominante no mercado. Contudo, o problema reside no fato de que tal alavancagem é indevida na medida em que os dados estão sem obtidos a partir do exercício de um poder assimétrico em face dos prestadores de serviço médico à jusante sem qualquer justificativa legal válida. Tais informações não poderiam ser obtidas por outros meios, na medida em que há um dever de sigilo desses dados.

Em outras palavras, o compartilhamento dessas informações favorece as grandes OPS, que podem se valer destas como um privilégio competitivo não natural. Desse modo, o compartilhamento de dados pode prejudicar ainda mais o processo concorrencial em um mercado já marcado por altas barreiras à entrada e tendência à concentração.

Essa questão torna-se mais sensível na medida em que, em atos de concentração mais recentes<sup>126</sup>, relevantes agentes do setor têm adquirido empresas atuantes em outros mercados verticalmente relacionados ou complementares, como aqueles de radiofármacos, corretagem de seguros, desenvolvimento de *softwares* de gestão de saúde e outros serviços de tecnologia da informação voltados à área da saúde. Assim, cresce-se a suspeita pelo uso indevido dos dados que podem adquirir uma vantagem competitiva ainda maior, ao serem combinados com outras informações advindas desses demais setores relacionados, ou ainda podem ser utilizados em favor de uma atuação anticompetitiva nesses outros setores também para o desenvolvimento de soluções mais eficientes nesses mercados, servindo como estratégia ilícita de alavancagem desses grandes conglomerados.

Portanto, a estrutura de mercado da cadeia suplementar descrita revela questões de preocupação concorrenciais na exigência de compartilhamento indevido de dados sensíveis de saúde contidos nos prontuários eletrônicos dos pacientes-beneficiários, principalmente quando essa exigência é feita por grandes grupos econômicos com presença abrangente ao longo da cadeia e outros mercados próximos.

---

126 “Acrescente-se que, nos últimos 4 anos, tem havido uma expansão por parte de importantes grupos da cadeia produtiva de saúde suplementar, sejam para mercados complementares, o que implica expansão de portfólio; sejam para outros mercados verticalmente relacionados, como os setores de radiofármacos, corretagem de seguros e desenvolvimento de softwares na área de gestão de saúde”. In: Cadernos do Cade: Atos de concentração nos mercados de planos de saúde, hospitais e medicina diagnóstica, p. 96. Disponível em: <[https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/estudos-economicos/cadernos-do-cade/Cadernos-do-Cade\\_AC-saude-suplementar.pdf](https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/estudos-economicos/cadernos-do-cade/Cadernos-do-Cade_AC-saude-suplementar.pdf)>

## 5. Considerações finais

No presente estudo foi examinada a pertinência da exigência, por parte de algumas Operadoras de Planos de Saúde, de compartilhamento, pelos hospitais, independentemente de consentimento pelo titular, de prontuários médicos eletrônicos, por vezes, como condição para o cadastramento dos estabelecimentos de saúde. Busca-se embasar tal exigência nos artigos 7º, VIII e 11, II, f, da LGPD (que autoriza o tratamento independentemente de consentimento para *“tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária”*), afirmando-se que seguradoras de saúde poderiam ser enquadradas como *“serviços de saúde”*, tendo em vista que oferecem gestão de cuidado e medicina preventiva aos beneficiários, além do que, o compartilhamento dos prontuários médicos seriam um veículo de interoperabilidade entre diferentes hospitais, o que aumentaria a eficiência, qualidade e continuidade do tratamento dos pacientes.

Para enfrentar o tema com o cuidado necessário, examinamos, primeiramente a pertinência da sugestão de introdução de programa de interoperabilidade por meio do compartilhamento de prontuários eletrônicos com seguradoras de saúde. Conforme a análise da experiência internacional, essa seria uma forma inusitada de implantação de interoperabilidade no atendimento médico, tendo em vista que, em todos os países

pesquisados, a interoperabilidade se dá no contexto de atendimento, ou seja, pelo acesso de profissionais de saúde e estabelecimentos de saúde atuando diretamente no procedimento de saúde do paciente do qual pretende obter a história clínica disponível. Tal metodologia é assentada justamente no pilar de proteção aos dados dos pacientes e preservação da privacidade, considerando ainda ser suficiente para os propósitos de prover atendimento eficiente e contínuo. Também a Estratégia de Saúde Digital para o Brasil 2020-2028 refere-se à interoperabilidade como fundamental para a saúde digital, tratando-a, porém, como uma integração entre estabelecimentos de saúde e profissionais de saúde apenas. Desse modo, a interoperabilidade por meio de OPSs é estranha à experiência internacional e ao modelo sinalizado pelo Ministério da Saúde no Brasil.

Não apenas a interoperabilidade via seguradoras privadas de saúde seria inusitado, como a hipótese de compartilhamento de prontuários médicos entre OPSs traria as seguintes desvantagens e riscos, conforme apontado neste estudo:

- i) *Distorção dos incentivos*: desloca a interoperabilidade para a fonte pagadora, o que concentra os incentivos na redução de custos e não na saúde do paciente;
- ii) *Problema de inclusão*: população atendida pelo SUS não obterá os benefícios de eficiência e continuidade do tratamento, gerando um problema de inclusão social;
- iii) *Conflitos entre standards técnicos*: diferentes OPSs podem utilizar padrões técnicos e terminologias distintas entre si, o que significaria uma interoperabilidade fragmentada e parcial;
- iv) *Distorções concorrenciais*: assimetria entre hospitais integrados a OPSs, que teriam informações sensíveis sobre seus concorrentes, e hospitais não integrados, sem acesso a informações concorrenciaismente relevantes.

Já os programas de incentivo à adoção de hábitos saudáveis e de controle e prevenção de saúde pelas OPSs referem-se também a serviços prestados por profissionais de saúde, remotamente ou em estabelecimentos de saúde, de modo que a OPS continua sendo intermediária do serviço sem necessidade de acesso a histórico clínico dos pacientes. O aspecto informativo desses programas, como orientações para vida saudável e mesmo o uso de aplicativos para coleta de informações acerca desses hábitos não justifica o compartilhamento de prontuários eletrônicos, devendo as seguradoras de saúde obter o consentimento dos beneficiários para o envio ou uso de informações clínicas, assim como qualquer outro serviço semelhante, que não seja exercido, por determinação regulatória ou obrigação legal, por médicos.

Por fim, foi identificado neste estudo que as bases legais para o tratamento de dados pessoais de saúde pelas OPS são:

- A) *Cumprimento de obrigação legal ou regulatória pelo controlador*, o que limita as informações a serem compartilhadas entre hospitais e seguradoras de saúde ao estritamente necessário para:



- 1) Verificação de Elegibilidade;
  - 2) Autorização de procedimentos;
  - 3) Comunicação de internação ou alta do beneficiário;
  - 4) Cobrança de serviços de saúde;
  - 5) Demonstrativos de retorno;
  - 6) Envio e recebimento de documentos necessários para solicitação, autorização e cobrança;
  - 7) Recurso de glosa;
  - 8) Comprovante presencial;
- A) *Consentimento pelo titular*, que deve ser expresso, informado, inequívoco e em cláusula separada do contrato de prestação de serviços ou em instrumento próprio (nos termos do art. 8º e art. 11 da LGPD).

Não se legitima o tratamento de dados pessoais, em particular o acesso a prontuários médicos, por seguradoras de saúde, com base no artigo 7º, VIII, ou no art. 11, II, alínea “f”, da LGPD. Isso porque seguradoras de saúde não constituem prestadoras de serviços de saúde, mas apenas intermediadoras de serviços de saúde prestados por terceiros (médicos e estabelecimentos de saúde). O ordenamento jurídico brasileiro, seja nas normas de tributação, seja nas normas setoriais de saúde, limita o conceito de prestadores de serviços de saúde a profissionais de saúde e estabelecimentos de saúde (hospitais, clínicas, laboratórios, ambulatórios). Uma vez que o inciso II do art. 11 se trata de norma de exceção ao dever de coletar o consentimento do titular, não cabe interpretação ampliativa para abarcar seguradoras de saúde nesse conceito. Ademais, as hipóteses versadas no inciso VIII do art. 7º e na alínea “f”, inciso II, do art. 11, dizem respeito ao contexto específico de um procedimento médico de atendimento ao paciente, o que não é congênere à atuação de uma OPS como intermediária financeira do serviço.

Por fim, com relação ao projeto de prontuário médico único, que centralizaria os dados de prontuários médicos de estabelecimentos de saúde públicos e privados nas mãos do Estado, o presente estudo aponta que a experiência internacional, com exceção da Inglaterra, segue a tendência oposta, no sentido de promover a interoperabilidade no acesso a dados por meio de padronização técnica e semântica, não de centralização da base de dados. Além disso, o estudo vislumbra óbices constitucionais, tendo em vista o princípio de separação de poderes informacional, corolário do direito fundamental à proteção de dados, bem como aponta riscos quanto à unidade informacional, em particular quanto ao impacto mais grave em incidentes de segurança e vazamento de dados.

Embora não haja detalhamento pelo Ministério da Saúde sobre a proposta de um modelo de *Open Health* para o Brasil, o presente estudo traz elementos suficientes para se descartar um modelo de transferência de dados de saúde entre operadoras de saúde, independentemente de consentimento de seus titulares, apontando que a portabilidade de dados entre operadoras deve ter como princípio o consentimento dos titulares. Todavia, um posicionamento mais assertivo sobre esse tema depende de maior detalhamento do projeto em questão.

## 5.1 Resumo do problema e das considerações finais

O presente estudo teve por objetivo responder à seguinte pergunta: as Operadoras de Planos de Saúde (OPS) teriam direito a receber dados de saúde constantes no prontuário médico sem o consentimento do usuário/paciente, com base no Art. 7º, VIII, e Art. 11, II, “f”, da LGPD?

O questionamento decorre, sobretudo, do fato de a Nota Técnica nº 3/2019/GEPIN/DIRAD-DIDES/DIDES da ANS, publicada em 21/11/2019, apresentar o entendimento de que o compartilhamento e tratamento de dados de saúde por OPSs não dependeria de consentimento, por encontrar fundamento na base legal apontada na alínea f, inc. II do art. 11 da LGPD (hipótese de dispensa de consentimento do titular no caso de tratamento de dados pessoais para tutela à saúde desde que “exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária”).

A conclusão a que se chega é de que não é legítimo o tratamento de dados pessoais, em particular o acesso a prontuários médicos, por seguradoras de saúde, com base no artigo 7º, VIII, ou no art. 11, II, alínea “f”, da LGPD. Isso porque seguradoras de saúde não constituem prestadoras de serviços de saúde, mas apenas intermediadoras de serviços de saúde prestados por terceiros (médicos e estabelecimentos de saúde). O ordenamento jurídico brasileiro, seja nas normas de tributação, seja nas normas setoriais de saúde, limita o conceito de prestadores de serviços de saúde a profissionais de saúde e estabelecimentos de saúde (hospitais, clínicas, laboratórios, ambulatórios). Uma vez que o inciso II do art. 11 se trata de norma de exceção ao dever de coletar o consentimento do titular, não cabe interpretação ampliativa para abarcar seguradoras de saúde nesse conceito. Ademais, as hipóteses versadas no inciso VIII do art. 7º e na alínea “f”, inciso II, do art. 11, dizem respeito ao contexto específico de um procedimento médico de atendimento ao paciente, o que não é congênere à atuação de uma OPS como intermediária financeira do serviço.

Embora a Estratégia De Saúde Digital Para O Brasil 2020-2028 estabeleça, dentre as 7 prioridades de seu plano de governança, a “informatização dos 3 Níveis de Atenção [à Saúde]” e a promoção de um “ambiente de interconectividade”, o estudo demonstrou que, com relação ao projeto de prontuário médico único, a experiência internacional, com exceção da Inglaterra, segue a tendência oposta, no sentido de promover a interoperabilidade no acesso a dados por meio de padronização técnica e semântica, não de centralização da base de dados. No que tange à criação de um modelo de *Open Health* para o país, o estudo traz elementos suficientes para se descartar um modelo de transferência de dados de saúde entre operadoras de saúde sem consentimento dos titulares dos dados, não obstante um posicionamento mais assertivo sobre esse tema dependa de maior detalhamento sobre um sistema de dados de saúde aberto.