[Código de Boas Práticas]

Proteção de Dados para Prestadores Privados em Saúde

CNSaúde
CONFEDERAÇÃO NACIONAL DE SAÚDE

EDIÇÃO 2021

[Código de Boas Práticas]

Proteção de Dados para Prestadores Privados em Saúde

[INICIATIVA]

CNSaúde
CONFEDERAÇÃO NACIONAL DE SAÚDE

[PARCEIROS]

ANS Agência Nacional de Saúde Suplementar
Rede D'Or São Luiz
MaterDei Rede de Saúde
sabin Medicina Diagnóstica
impar
dasa

FENAESS Federação Nacional dos Estabelecimentos de Serviços de Saúde
FEHOSPAR
FEHOESP Federação dos Hospitais, Clínicas e Laboratórios do Estado de São Paulo
FEBASE Federação Baiana de Saúde
FEHERJ Federação dos Hospitais e Estabelecimentos de Serviços de Saúde do Estado do Rio de Janeiro
FEHOESG Federação dos Hospitais do Estado de Goiás
FEHOESC Federação dos Hospitais e Estabelecimentos de Serviços de Saúde do Estado de Santa Catarina
FEHOSUL Federação dos Hospitais e Estabelecimentos de Saúde do Rio Grande do Sul

Equipe

CNSaúde
Breno de Figueiredo Monteiro – Presidente
Bruno Sobral de Carvalho – Sec. Executivo
Marcos Vinícius Ottoni – Coordenador Geral Jurídico
Joicy Damares – Coordenadora Jurídica
Clóvis Queiroz – Coord. Geral Rel. de Trabalho e Sindical
Claudia Silva – Coordenadora Financeira

Coordenação científica e redação:
Laura Schertel Mendes – Coordenadora Científica
Danilo Doneda – Coordenador Científico
Marcos Vinícius Ottoni – Coordenador Executivo
Mônica Tiemy Fujimoto - Redação
Walquiria Favero - Rede Impar/DASA - Revisão
Luiz Gustavo Homrich – ANS - Revisão

Membros do Grupo de Trabalho
Fábio Cunha – Rede Impar/DASA
Ianno Soares – MaterDei Rede de Saúde
Jonas Pulcheri – Rede D'Or São Luiz
Júlio Tinoco - ANS
Leandro Rezende – Rede D'Or São Luiz
Lidia Abdalla – Grupo Sabin
Lourivana Lima – Grupo Sabin
Maria Fernanda Carvalho – MaterDei Rede de Saúde

Introdução

A Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/18) entrou em vigor em setembro de 2020, após 8 anos de intensos debates sobre privacidade e proteção de dados no país. Com a sua aprovação, o Brasil passa a ter uma legislação moderna e específica sobre o tema, com novas regras que objetivam proteger a privacidade e intimidade do indivíduo, mediante a definição de princípios, direitos e deveres para o tratamento de dados pessoais no Brasil.

A LGPD criou a Autoridade Nacional de Proteção de Dados – ANPD, regulamentada pelo Decreto nº 10.474/2020, que é o órgão responsável pela supervisão da lei, por elaborar as diretrizes para a Política Nacional de Proteção de Dados Pessoais e Privacidade e promover a regulamentação dos setores que lidam com dados pessoais. Entre as funções da ANPD está a de coordenar as ações com os órgãos e entidades responsáveis por setores específicos da atividade econômica para promover o seu adequado funcionamento, conforme as disposições regulamentares e a legislação.

O início da vigência da LGPD é, portanto, um marco significativo para a consolidação dos direitos e garantias fundamentais do indivíduo, com forte impacto sobre todos os setores da sociedade. O setor de saúde, por envolver um enorme fluxo de tratamento de dados pessoais sensíveis, merece um olhar aprofundado e específico sobre o tema.

Diante disso, considerando a vigência da Lei, a centralidade do fluxo de dados no setor de saúde e a importância de garantir a confiança do cidadão na proteção de dados nesse setor, a Confederação Nacional de Saúde - CNSaúde iniciou, em 2019, estudos preliminares de prática regulatória, no que pertine ao tratamento de dados pessoais, com o objetivo de propor a criação de um Código de Boas Práticas, de forma a melhor contribuir com a implementação da LGPD pelos prestadores privados de saúde suplementar.

Assim, foi criado o Grupo de Trabalho pela CNSaúde, em conjunto com a Rede Ímpar/DASA, o Grupo Sabin, a Rede D'Or São Luiz e a MaterDei Rede de Saúde, representando Hospitais Gerais e entidades de Medicina Diagnóstica. O referido Grupo de Trabalho foi estruturado sob a Coordenação Executiva do Coordenador Geral Jurídico da CNSaúde, Marcos Vinícius Ottoni.

Para exercer a Coordenação Científica do Grupo de Trabalho foram convidados a professora Laura Schertel Mendes e o professor Danilo Doneda, que contaram com a colaboração técnica de Mônica Tiemy Fujimoto.

Outrossim, o ingresso e a efetiva participação da Agência Nacional de Saúde Suplementar – ANS foi de fundamental importância para a elaboração do presente Código, diante do seu largo conhecimento do setor e da já destacada prática regulatória de excelência.

Vale lembrar que os desafios de implementação da legislação sobre proteção de dados encontram-se atualmente no centro da discussão econômica e política no mundo, e igualmente no Brasil.

Hoje está claro que o Estado tem muito a ganhar se puder contar com a colaboração da sociedade para compartilhar a responsabilidade de implementar sua agenda regulatória - em particular diante de todas as complexidades advindas das novas aplicações tecnológicas, despontando como fundamental o apoio d rede de atores privados que formula, desenha, utiliza e aplica essas tecnologias.

É nesse sentido que a LGPD traz, de forma inovadora, a possibilidade de realização de códigos de conduta pelo setor privado, nos termos de sua seção II, dedicada exclusivamente às boas práticas e à governança. O seu art. 50, caput, traz a possibilidade de que as empresas individualmente ou por meio de associações formulem regras de boas práticas e de governança, enquanto o parágrafo 3º deste mesmo dispositivo estabelece a possibilidade de que

tais regras sejam reconhecidas e divulgadas pela Autoridade Nacional.

A CNSaúde entende que a referida inovação legislativa constitui uma grande oportunidade para o setor promover a implementação da LGPD, aplicando as melhores práticas nacionais e internacionais e garantindo os direitos previstos no referido diploma legal, ao tempo que possibilita debater as suas especificidades como um setor amplamente regulado, dependente do fluxo de dados em toda a cadeia de operadores de saúde e ainda marcado por um altíssimo grau de inovação.

Trata-se, portanto, de verdadeiro marco de governança e boas práticas, visto que o texto se apresenta como o primeiro Código de Conduta dos Prestadores do Serviço de Saúde para atendimento à LGPD. A iniciativa, além de orientar quanto às condutas a serem praticadas por hospitais e laboratórios privados, visa incentivar a inovação com responsabilidade e consolidar a confiança dos titulares de dados no setor de saúde.

Brasília, 12 de março de 2021

Breno de Figueiredo Monteiro
Presidente CNSaúde

Código de Boas Práticas de Proteção de Dados para os Prestadores Privados em Saúde

Sumário

Parte I

Protocolos

Parte II

PARTE I

1. Considerações iniciais

A Confederação Nacional de Saúde, Hospitais, Estabelecimentos e Serviços (CNSaúde) é uma entidade sindical fundada em 1996 que representa a totalidade dos estabelecimentos de serviços de saúde no país, incluindo hospitais, clínicas, casas de saúde, laboratórios de análises clínicas e patologia clínica, serviços de diagnóstico, imagem e fisioterapia, entre outros do gênero.

O setor de saúde realiza, pela sua própria natureza, tratamentos de dados pessoais de forma intensa, seja para a realização de procedimentos clínicos, para a pesquisa clínica e científica, bem como para possibilitar a interoperabilidade entre os diversos atores do sistema de saúde com o máximo grau de eficiência.

Tendo a atenção com a pessoa como seu objetivo último, abrangendo todos os aspectos da atuação do profissional de saúde, a preocupação com a utilização de informações pessoais sempre esteve presente no setor - aluda-se, simbolicamente, ao trecho final do juramento hipocrático: "Sobre aquilo que vir ou ouvir respeitante à vida dos doentes, no exercício da minha profissão ou fora dela, e que não convenha que seja divulgado, guardarei silêncio como um segredo religioso".

A consciência do papel fundamental da informação pessoal no setor de saúde, presente desde sempre, é também objeto de constante evolução, na medida em que as tecnologias de informação e comunicação vêm, com muita intensidade, criando possibilidades nas frentes clínica, de

pesquisa e administrativa no setor, a ponto de redefinir vetores tradicionais e vislumbrar novas possibilidades.

Para o pleno desenvolvimento destas novas possibilidades, bem como para que os processos já implementados, e que se utilizam de dados pessoais, se consolidem com segurança, aderência à legislação e proporcionem total confiança aos cidadãos e a sociedade, passa a ser imperativo que o setor considere e se adapte ao modelo regulatório geral sobre proteção de dados pessoais introduzido, no Brasil, pela Lei Geral de Proteção de Dados (LGPD).

A LGPD, na esteira de legislações similares hoje presente em quase 150 países, reconhece a relevância da informação pessoal para o indivíduo e a sociedade, proporcionando a este, ferramentas e estruturas para que possa controlar o uso de seus dados com maior transparência e eficiência e, àquela, condições para que os dados pessoais possam ser legitimamente utilizados em um ambiente de confiança.

A introdução deste marco regulatório de natureza geral implica na necessidade da adaptação de todas as atividades que realizem tratamento de dados pessoais, incluindo o setor de saúde. Mesmo considerando uma forte tradição de respeito aos dados pessoais já existente no setor, consubstanciado tanto no sigilo médico, nos critérios éticos levados em conta na pesquisa e em tantos outros, surge a necessidade de que o tratamento de dados no setor opere de forma harmônica com todos os outros setores, implementando conceitos, princípios e procedimentos que irão uniformizar o tratamento de dados pessoais para o benefício do cidadão e também com um potencial e expressivo ganho em termos de confiança e interoperabilidade, entre outros.

Um dos recursos mais eficazes para a adequação aos marcos normativos de proteção de dados é a estipulação de normas deontológicas no setor, que se consubstanciam em Códigos de Conduta ou Guias de Melhores Prática. Estes buscam aplicar as normas gerais de proteção de dados pessoais às hipóteses específicas de tratamento de dados de cada setor, bem como as melhores práticas adotadas, de modo a sistematizar um conjunto de medidas a serem adotadas pelo setor como um todo. Com isso, firma-se um compromisso público de que, além do cumprimento da legislação em si, o setor se compromete às medidas adicionais e específicas para a sua realidade constantes no documento.

2. A Lei Geral de Proteção de Dados (LGPD)

A Lei 13.709/2018 (Lei Geral de Proteção de Dados) determina o perfil a ser adotado para os tratamentos de dados pessoais em todos os setores, estabelecendo conceitos e instrumentos que estarão presentes em toda a discussão sobre a matéria. De certa forma, ela estabelece, pela primeira vez no Brasil, uma gramática e um campo conceitual de referência em torno do qual toda a discussão sobre o tema - inclusive o Guia de Boas Práticas que é objeto de nosso trabalho, irá se orientar.

A entrada em vigor da LGPD institui um regime geral de proteção de dados no ordenamento brasileiro, a partir de um conceito amplo do dado pessoal e do seu tratamento, submetendo todos os dados pessoais ao seu regime de tutela.

2.1. Princípios de proteção de dados pessoais

Os princípios da proteção de dados, presentes no art. 6º, LGPD fornecem parâmetros fundamentais para nortear o tratamento de dados e que são concretizados pelos dispositivos legais subsequentes:

I. **Boa-fé objetiva**: presente no caput do art. 6º e que ressalta a necessidade de que os tratamentos de dados pessoais sejam pautados pelo caráter cooperativo e lisura, que deve ser passível de constatação a partir de atos objetivos.
II. **finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
III. **adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
IV. **necessidade**: 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;
V. **livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
VI. **qualidade dos dados**: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VII. **transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos

agentes de tratamento, observados os segredos comercial e industrial;

VIII. **segurança**: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

IX. **prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

X. **não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

XI. **responsabilização e prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

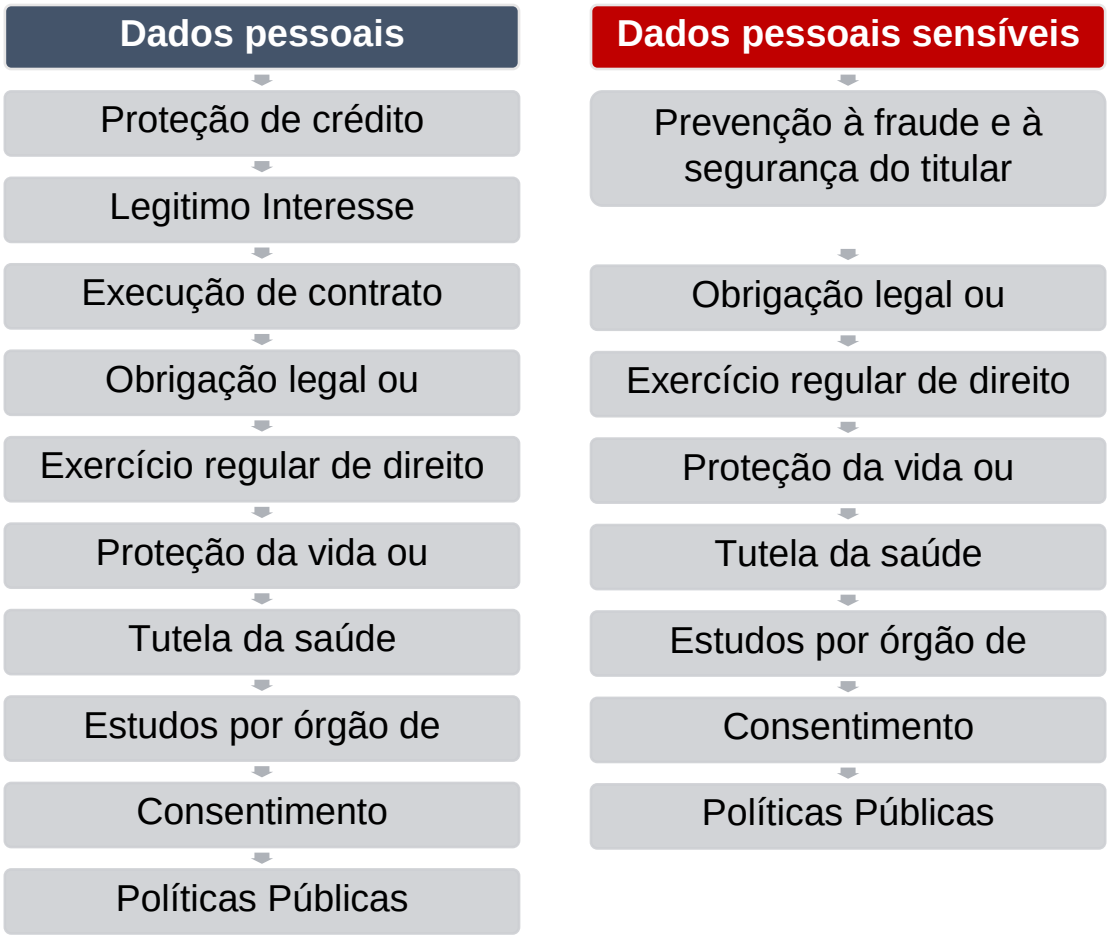
2.2. Bases legais para o tratamento de dados pessoais

A lei representa um avanço na proteção de dados ao prever condições de legitimidade para o tratamento de dados pessoais. De acordo com a LGPD, portanto, todo tratamento de dados pessoais deve estar amparado por uma das bases legais presentes em seu artigo 7º, entre as quais o consentimento do titular, a execução de um contrato, a proteção da vida, a tutela da saúde, o legítimo interesse, entre outros (MENDES, 2019).

O setor de saúde deve observar, ainda, cuidado adicional, tendo em vista que a legislação confere proteção

diferenciada para os dados considerados sensíveis[1], dentre os quais se incluem os dados de saúde, cuja proteção é feita em maior medida pela lei, inclusive quanto a um rol diferenciado de bases legais disponíveis para o seu tratamento (art. 11).

[1] "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; oug) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais".



Tanto quanto as condições de legitimidade, os princípios devem também ser criteriosamente considerados no tratamento de dados. Por exemplo, ainda que a base legal utilizada seja a da "execução de contrato", os dados tratados para o seu cumprimento devem atender, por exemplo, aos princípios da necessidade e finalidade (art. 6, I e III, LGPD). De igual modo, ainda que um dado pessoal seja tratado com o consentimento de seu titular, o tratamento não pode ser realizado para fins discriminatórios, ilícitos ou abusivos (art. 6, IX, LGPD).

Especial atenção merece a base legal da tutela da saúde, que está apta a autorizar o tratamento tanto de dados sensíveis, como de dados não sensíveis. Para utilização dessa base é necessário cautela, tendo em vista que seu conceito não se aplica indiscriminadamente a todas as etapas da prestação de serviços de saúde. Assim, sugere-se

que a sua utilização seja realizada à luz do conceito de tutela da saúde presente no Artigo 9(2)(h) e Artigo 9(3) do Regulamento Geral sobre a Proteção de Dados da União Europeia (RGPD) :

> 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, sob reserva das condições e garantias previstas no nº 3;
> (...)
> 3. Os dados pessoais referidos no nº 1 podem ser tratados para os fins referidos no nº 2, alínea h), se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes.

Ou seja, ainda que a uma primeira vista a tutela da saúde pareça ser a base legal aplicável à maioria dos processos de tratamento do setor de saúde, é necessário distinguir quais tratamentos são realizados no âmbito das atividades fim dos prestadores (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) e por profissionais de saúde sujeitos à obrigação de sigilo. Caso contrário, a base legal "tutela da saúde" pode não ser a mais adequada.

2.3. Direitos dos titulares

A LGPD também prevê determinados procedimentos que devem ser assegurados para garantir a proteção dos direitos dos titulares, bem como o seu legítimo exercício. Os direitos básicos atribuídos ao titular pelas diversas legislações nacionais e tratados internacionais para o controle do fluxo de seus dados são conhecidos pela sigla "ARCO", abreviação de: acesso, retificação, cancelamento e oposição (MENDES, 2019).

Outros diplomas normativos brasileiros contêm direitos para o cidadão sobre seus dados. Por exemplo, o Código de Defesa do Consumidor ("CDC") procura proteger os direitos do consumidor sobre seus próprios dados pessoais, em particular quando presentes em bancos de dados de proteção ao crédito[2]. O Marco Civil da Internet[3], por sua vez, estabelece uma série de prerrogativas e direitos aos usuários da Internet sobre seus próprios dados. Uma tutela de escopo mais amplo, porém igualmente voltada para a proteção de dados pessoais, pode ser observada no próprio Código Civil, incidindo a partir da proteção dos direitos de personalidade e da tutela dos direitos subjetivos (DONEDA, 2019).

A LGPD estabelece, além dos chamados direitos ARCO, uma série de outros direitos para o titular, entre os quais assume particular relevância o direito de portabilidade. A portabilidade dos dados pessoais, direito derivado do poder geral de controle do titular sobre seus dados, implica na necessidade do controlador implementar mecanismos que possibilitem a passagem dos dados pessoais para outros

[2] Art. 43, Lei 8.078/1990 (CDC): "O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes".
[3] Lei 12.965/2014.

controladores, mediante requisição do titular. Tal possibilidade, essencialmente dependente de um determinado nível de interoperabilidade entre diversos controladores, deve aguardar regulamentação da ANPD para que possa operar, porém se destaca sua potencial importância no setor de saúde, ao se considerar as possibilidades do titular escolher e mudar controladores à medida em que deseje mudar de prestador de serviços de saúde - como, particularmente, serviços de *eHealth.*

2.4. Agentes do tratamento

Outro aspecto da lei que merece atenção é a criação da figura dos agentes de tratamento de dados, de forma compatível com diversos outros marcos normativos congêneres, como, por exemplo, o europeu (RGPD)[4].

Os agentes de tratamento que, pela LGPD são o controlador e o operador, são os únicos sujeitos que realizam operações de tratamento de dados e, de acordo com sua atuação, podem ser considerados responsáveis em caso de descumprimento da legislação. Dentre as obrigações dos agentes de tratamento, destaca-se a obrigatoriedade de adoção de medidas de segurança, técnicas e administrativas para proteção de acessos não autorizados; o registro das operações de tratamento de dados e a elaboração de relatório de impacto.

[4] Quanto às figuras de agentes do tratamento, uma referência muito importante é o documento técnico "Opinion 1/2010 on the concepts of controller and processor", recepcionado elo EBPB (*European Data Protection Board*) em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

2.5. Obrigações dos agentes de tratamento

Para além dos direitos dos titulares, a LGPD atribui aos agentes de tratamento uma série de obrigações que devem ser cumpridas durante o tratamento de dados pessoais, em especial, a obrigação de indicar o encarregado de tratamento de dados pessoais (art. 41), de manter a segurança da informação em todos os tratamentos (art. 46 e ss.) e de realizar o registro do tratamento de dados (art. 37).

2.6. Segurança da informação

A obrigação de manter a segurança da informação permeia as obrigações previstas em detalhes nos protocolos da Parte II, contudo, ressalta-se que qualquer que seja a hipótese de tratamento, os dados devem ser mantidos em ambiente controlado e seguro, adotando, sempre que possível, anonimização ou pseudonimização dos dados, nos termos dos arts. 46 e ss.

2.7. Autoridade de garantia e regime sancionatório

Enquanto, por um lado, os dados pessoais acarretam benefícios sociais, aumento do valor das empresas, serviços públicos mais eficientes e aumento da qualidade do serviço prestado ao consumidor. Por outro lado, caso o tratamento dos dados seja feito de forma inadequada - e sem considerar os princípios e regras que constam na LGPD -, os agentes controladores e operadores[5] do tratamento de dados podem ser responsabilizados.

[5] Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Já as penalidades passíveis de serem aplicadas se encontram no art. 52 da mesma lei, podendo ser mencionadas a possibilidade de advertência, aplicação de multa de até 50 milhões ou mesmo a suspensão parcial ou total das atividades que envolvem o tratamento de dados:

> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Daí porque se entende que a ANPD figura como autoridade de garantia do cumprimento da LGPD, zelando pela proteção dos dados pessoais nos termos da legislação.

2.8. Boas práticas e governança

Para a consideração, em sua plenitude, do arcabouço regulatório da proteção de dados no direito brasileiro, necessário considerar a LGPD, bem como normativas que se relacionem com a matéria como o CDC, o Marco Civil da Internet, a Lei de Acesso à Informação, regulamentações setoriais aplicáveis, entre outras. Ante a complexidade do

tema e a existência de conceitos abertos, a aplicação efetiva da legislação deve ser adaptada aos aspectos individuais dos agentes, considerando devidamente os riscos e o arcabouço regulatório (FRAZÃO, 2019).

Daí a importância do reconhecimento do modelo regulatório híbrido da Proteção de dados, utilizando-se os Códigos de Conduta como uma forma de buscar coordenar as diversas normativas que incidem particularmente sobre um determinado setor ou atividade, sob a lógica e gramática da LGPD. Tal prática proporciona a complementariedade entre os instrumentos jurídicos existentes (ZANATTA, 2015) e concretiza a autorregulação prevista no art. 50 da LGPD.

Especificamente em relação ao setor de saúde, além do cumprimento com os requisitos da LGPD, o setor é dotado de regulação e dinâmica própria, de modo que a sua aplicação deve observar tais características. Por esse motivo, o presente guia será dividido em duas partes. A primeira parte se destinará a explorar o marco normativo que permeia o encontro entre a proteção de dados e a regulação setorial, bem como analisará a atuação das agências regulatórias. Ademais, também trataremos dos principais conceitos da LGPD, do âmbito de aplicação do guia, considerando o ciclo de vida típico dos dados no setor conforme fluxograma.

A segunda parte estabelecerá protocolos para as questões mais sensíveis do setor, quais sejam:

1. Protocolo de atendimento
2. Protocolo de compartilhamento
3. Protocolo de pesquisa clínica
4. Protocolo para exercício dos direitos dos titulares
5. Protocolo de Segurança da Informação

Este Guia de Boas Práticas da CNSaúde foi elaborado em conjunto por especialistas da área de proteção de dados, com membros da Agência Nacional de Saúde Suplementar - ANS e representantes dos prestadores do setor, com o objetivo de colaborar com a Agência Nacional de Proteção de Dados (ANPD) e outros entes da administração pública na aplicação da LGPD no setor privado de saúde, estabelecendo um marco autorregulatório a ser seguido. Por meio deste documento busca-se a confluência das especificidades normativas já existentes na prestação de serviços de saúde e a efetividade da proteção de dados, nos termos do previsto no art. 50 da LGPD.

3. Definições[6]

Agentes de tratamento: o controlador e o operador;

Agência Nacional de Saúde Suplementar (ANS): Autarquia, sob regime especial, que atua em todo o território nacional, como órgão de regulação, normatização, controle e fiscalização das atividades que garantem a assistência suplementar à saúde.

Autorização prévia de procedimento de saúde: mecanismo de regulação da operadora que consiste em avaliação da solicitação antes da realização de determinados procedimentos de saúde.

Atividades de Apoio Diagnóstico e Terapêutico (SADT): abrange as diversas atividades de apoio diagnóstico e/ou

[6] Definições extraídas da LGPD, do Marco Civil da Internet, Glossário ANS (2012) e Glossário do Ministério da Saúde (2004), Manual de Conceitos Básicos da Saúde para produtos DATASUS (2000), Manual de Certificação para Sistemas de Registro Eletrônico em Saúde elaborado pelo SBIS (2020) e do portal eletrônico do CNS (disponível em: https://conselho.saude.gov.br/Web_comissoes/conep/aquivos/conep/atribuicoes.html) .

terapêutico, tais como: laboratórios de análises clínicas, anatomia patologia, radiologia, endoscopia, fisioterapia, provas funcionais, hemoterapias, traçados diagnósticos (EEG, ECG) e os atendimentos individuais e em grupos realizados pelas diversas categorias profissionais nas unidades de saúde.

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

Beneficiário: beneficiário de plano privado de assistência à saúde.

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Comitês de Ética em Pesquisa (CEP) - Comitês organizados nas instituições onde as pesquisas envolvendo seres humanos se realizam, para revisar todos os protocolos de pesquisa, cabendo-lhe a responsabilidade primária pelas decisões sobre a ética da pesquisa a ser desenvolvida na instituição, de modo a garantir e resguardar a integridade e os direitos dos voluntários participantes nas referidas pesquisa;

Comissão Nacional de Ética em Pesquisa (CONEP): Comissão do Conselho Nacional de Saúde - CNS, criada com a função de implementar as normas e diretrizes regulamentadoras de pesquisas envolvendo seres humanos, aprovadas pelo Conselho.

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

Ensaios clínicos: Qualquer pesquisa que, individual ou coletivamente, envolva o ser humano, de forma direta ou indireta, em sua totalidade ou partes dele, incluindo o manejo de informações ou materiais.

Hospital: Estabelecimentos de Saúde destinado a prestar assistência médica e hospitalar a pacientes em regime de internação.

Internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes.

Instituição de pesquisa: Organização pública ou privada, legitimamente constituída e habilitada na qual são realizadas investigações científicas.

Operadora de saúde: Pessoa jurídica constituída sob a modalidade de sociedade civil ou comercial, cooperativa, ou entidade de autogestão, que opere produto, serviço ou contrato de Plano Privado de Assistência à Saúde, assim como descrito na Lei n.º 9.656, de 3 de junho de 1998.

Padrão de Troca de Informação em Saúde Suplementar: Padrão TISS. Padrão obrigatório para o registro e troca de informações na Saúde Suplementar dos eventos do ciclo de atenção à saúde realizados em beneficiários de planos privados de assistência à saúde.

Pesquisa em saúde: Pesquisas cujos resultados são aplicados no setor Saúde, voltados, em última instância, para a melhoria da saúde de indivíduos ou grupos populacionais. Podem ser categorizadas por níveis de atuação científica e compreendem os tipos de pesquisa básica, clínica, epidemiológica e avaliativa, além de pesquisa em outras áreas como economia, sociologia, antropologia, ecologia, demografia e ciências.

Plano de saúde: O Plano Privado de Assistência à Saúde é uma prestação continuada de serviços ou coberturas de custos assistenciais a preço pré ou pós-pago, por prazo indeterminado, com a finalidade de garantir, sem limite financeiro, a assistência à saúde, pela faculdade de acesso e atendimento por profissionais e 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 do prestador, por conta e ordem do consumidor.

Prestadores privados de serviço de saúde – são considerados os prestadores privados de serviços de saúde os profissionais de saúde os estabelecimentos que realizam serviços de saúde.

Prontuário médico: conjunto de documentos padronizados, destinados ao registro da assistência prestada ao paciente.

Protocolo de pesquisa: Documento contemplando a descrição da pesquisa em seus aspectos fundamentais, informações relativas ao sujeito das pesquisas, à qualificação dos pesquisadores e a todas as instâncias responsáveis.

Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

Rede de prestadores de serviços de saúde da operadora de planos privados de assistência à saúde: Rede de serviços de saúde contratada, referenciada ou credenciada, de forma direta ou indireta; e Rede própria da operadora; de entidade

ou empresa controlada pela operadora; de entidade ou empresa controladora da operadora e profissional assalariado ou cooperado da operadora.

Serviços de Saúde: estabelecimentos destinados a promover a saúde do indivíduo, protegê-lo de doenças e agravos, prevenir e limitar os danos a ele causados e reabilitá-lo quando sua capacidade física, psíquica ou social for afetada.

Sistema de Registro Eletrônico de Saúde (S-RES) - sistema que capture, armazene, apresente, transmita ou imprima informação identificada em saúde. Entende-se por informação identificada aquela que permite individualizar um paciente, o que abrange não apenas o seu nome, mas também números de identificação (tais como RG e CPF etc.) ou outros dados que, se tomados em conjunto, possibilitem a identificação do indivíduo

Terminal: o computador ou qualquer dispositivo que se conecte à internet.

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados,

reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

4. Marco normativo

- Lei nº 8.078, de 11 de setembro de 1990 - Dispõe sobre a proteção do consumidor.
- Lei nº 8.080, de 19 de setembro de 1993 - Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências
- Lei nº 9.656, de 3 de junho de 1998 - Dispõe sobre os planos e seguros privados de assistência à saúde.
- Lei nº 9.782, de 26 de janeiro de 1999 - Define o Sistema Nacional de Vigilância Sanitária, cria a Agência Nacional de Vigilância Sanitária, e dá outras providências.
- Lei nº 9.961 de 28 de janeiro de 2000 - Cria a Agência Nacional de Saúde Suplementar – ANS e dá outras providências.
- Lei nº 12.965, de 23 de abril de 2014 - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
- Lei nº 13.787, de 27 de dezembro de 2018 - Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.
- Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).
- Lei nº 13.979, de 6 de fevereiro de 2020 - Dispõe sobre as medidas para enfrentamento da emergência de

saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019.

- Lei nº 14.063, de 23 de setembro de 2020 - Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de *softwares* desenvolvidos por entes públicos.

Resoluções Normativas e Súmulas Normativas da ANS

- RN nº 255, de 18 de maio de 2011 - Dispõe sobre a designação do responsável pelo fluxo das informações relativas à assistência prestada aos beneficiários de planos privados de assistência à saúde.
- RN nº 305, de 9 de outubro de 2012 - estabelece o Padrão obrigatório para Troca de Informações na Saúde Suplementar - Padrão TISS dos dados de atenção à saúde dos beneficiários dos Planos Privados de Assistência à Saúde.
- RN nº 389, de 26 de novembro de 2015 - Dispõe sobre a transparência das informações no âmbito da saúde suplementar, estabelece a obrigatoriedade da disponibilização do conteúdo mínimo obrigatório de informações referentes aos planos privados de saúde no Brasil.
- Súmula Normativa nº 27, de 10 de junho de 2015 – veda a prática de seleção de riscos pelas operadoras de planos de saúde na contratação de qualquer modalidade de plano privado de assistência à saúde.

Resoluções da Diretoria Colegiada da Anvisa

- RDC nº 9, de 20 de fevereiro de 2015 - Dispõe sobre o Regulamento para a realização de ensaios clínicos com medicamentos no Brasil.
- RDC nº 10, de 20 de fevereiro de 2015 - Dispõe sobre o regulamento para a realização de ensaios clínicos com dispositivos médicos no Brasil.

Resoluções do CFM

- Resolução CFM nº 1.605, de 15 de setembro de 2000 – Proíbe que o médico revele o conteúdo do prontuário ou ficha médica sem o consentimento do paciente.
- Resolução CFM nº 1.638, de 9 de agosto de 2002 - Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde.
- Resolução CFM nº 1.643, de 26 de agosto de 2002 (reestabelecida pela Resolução CFM nº 2.228 de 26 de fevereiro de 2019) - Define e disciplina a prestação de serviços através da Telemedicina.
- Resolução CFM nº 1.821, de 23 de novembro de 2007 - Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde.
- Resolução CFM nº 1.819, de 22 de maio de 2007 - Proíbe a inclusão do diagnóstico codificado (CID) ou tempo de doença no preenchimento das guias da TISS de consulta e solicitação de exames de seguradoras e operadoras de planos de saúde concomitantemente com a identificação do paciente.

- Resolução CFM nº 2.217, de 27 de setembro de 2018 – Código de Ética Médica.
- Resolução CFM nº 2.107, de 17 de dezembro de 2014 - Define e normatiza a Telerradiologia.

Ministério da Saúde

- Resolução CNS nº 251, de 07 de agosto de 1997 - Diretrizes e Normas Regulamentadoras de Pesquisa Envolvendo Seres Humano
- Resolução CNS nº 466, de 12 de dezembro de 2012 - incorpora referenciais da bioética, tais como, autonomia, não maleficência, beneficência, justiça e equidade, dentre outros, e visa a assegurar os direitos e deveres que dizem respeito aos participantes da pesquisa, à comunidade científica e ao Estado.
- Norma Operacional CONEP nº 001/2013 - organização e funcionamento do Sistema CEP/CONEP, e sobre os procedimentos para submissão, avaliação e acompanhamento da pesquisa e de desenvolvimento envolvendo seres humanos no Brasil.
- Portaria nº 589, de 20 de maio de 2015 - Institui a Política Nacional de Informação e Informática em Saúde (PNIIS).
- Resolução CNS nº 506, de 3 de fevereiro de 2016 - estabelece os critérios para o processo de acreditação de CEP do Sistema CEP/Conep, em instituições públicas e privadas. A tramitação do protocolo terá como base a gradação e a tipificação dos riscos definidas em norma própria, com critérios estabelecidos pela Comissão Nacional de Ética em Pesquisa (Conep), decorrentes das atividades de pesquisa envolvendo seres humanos.
- Portaria nº 2.022, de 7 de agosto de 2017 - Altera o Cadastro Nacional de Estabelecimentos de Saúde

(CNES), no que se refere à metodologia de cadastramento e atualização cadastral, no quesito Tipo de Estabelecimentos de Saúde.

- Portaria nº 467, de 20 de março de 2020 - Dispõe, em caráter excepcional e temporário, sobre as ações de Telemedicina, com o objetivo de regulamentar e operacionalizar as medidas de enfrentamento da emergência de saúde pública de importância internacional previstas no art. 3º da Lei nº 13.979, de 6 de fevereiro de 2020, decorrente da epidemia de COVID-19.

5. Regulação setorial

Na prestação de Serviços de Saúde existem instituições centrais para a regulação setorial que, mesmo antes da entrada em vigor da LGPD, já vinham se preocupando com a proteção de dados de saúde. Não à toa, esses órgãos observam dispositivos normativos que auxiliam na proteção de dados do usuário. Dentre eles, destacamos: i) Agência Nacional de Saúde Suplementar - ANS; ii) Agência Nacional de Vigilância Sanitária - Anvisa e iii) Conselho Federal de Medicina - CFM.

Passa-se, portanto, à análise do papel dessas instituições na proteção de dados do usuário, bem como de seus principais dispositivos a respeito do assunto.

5.1. Agência Nacional de Saúde – ANS

A Agência Nacional de Saúde Suplementar é a agência reguladora vinculada ao Ministério da Saúde responsável pelo setor de planos e seguros privados de assistência à saúde. Criada pela Lei nº 9.961 de 28 de janeiro de 2000, a

agência possui diversas funções que se relacionam com a efetivação dos princípios e finalidades da proteção de dados.

Como exemplo, é possível mencionar as seguintes competências da ANS: a competência para estabelecer características dos instrumentos contratuais utilizados na atividade das operadoras (art. 4º, II, Lei nº 9.961/2000); estabelecer normas relativas à adoção e utilização, pelas operadoras de planos de assistência à saúde, de mecanismos de regulação do uso dos serviços de saúde (art. 4º, VII, Lei nº 9.961/2000); de estabelecer critérios, responsabilidades, obrigações e normas de procedimento para garantia dos direitos assegurados (art. 4º, XI, Lei nº 9.961/2000); de estabelecer normas, rotinas e procedimentos para concessão, manutenção e cancelamento de registro dos produtos das operadoras de planos privados de assistência à saúde (art. 4º, XVI, Lei nº 9.961/2000); proceder à integração de informações com os bancos de dados do Sistema Único de Saúde (art. 4º, XIX, Lei nº 9.961/2000).

Como já foi mencionado neste guia, um dos principais pontos de atenção com os dados de saúde é justamente a proteção dos titulares, de modo que a possibilidade da agência estabelecer normas de regulação do uso de serviços de saúde e garantia dos direitos dos titulares acaba por reforçar diretamente esse objetivo. Tal preocupação foi ressaltada na NOTA TÉCNICA Nº 3/2019/GEPIN/DIRAD-DIDES/DIDES (Processo nº 33910.029786/2019-51 da ANS), que envidou esforços para implementar os requisitos da LGPD na ANS, tendo em vista que a agência pode se enquadrar como controladora de dados a depender da situação.

Nesse mesmo sentido, ressaltam-se iniciativas como a criação do Comitê de Padronização das Informações em

Saúde Suplementar – COPISS, que mesmo antes da entrada em vigor da LGPD, se preocupava com os procedimentos de troca de dados de atenção à saúde no setor. O COPISS é composto por representantes da ANS, Ministério da Saúde, das operadoras de planos privados de assistência à saúde, dos prestadores de serviços de saúde, das instituições de ensino e pesquisa e das entidades representativas de usuários de planos privados de assistência à saúde; que estabeleceu o padrão obrigatório para Troca de Informações na Saúde Suplementar – TISS por meio da Resolução Normativa nº 305.

O padrão TISS[7] abrange a troca de dados de atenção à saúde entre operadoras de planos privados de assistência à saúde, prestadores de serviços de saúde e contratantes e beneficiários de planos privados de assistência à saúde, e tem como objetivo padronizar as ações administrativas, subsidiar as ações de avaliação e acompanhamento econômico, financeiro e assistencial das operadoras de planos privados de assistência à saúde e compor o Registro Eletrônico de Saúde. O protocolo tem como diretriz a interoperabilidade entre sistemas de informação da ANS, Ministério da Saúde e a redução das assimetrias de informação com os beneficiários de planos privados de assistência à saúde, sendo dividido nos seguintes componentes:

[7] Padrão TISS – Componente Organizacional. Outubro/2020.

Fonte: Padrão TISS – Componente Organizacional. Outubro/2020.

Tal iniciativa é de extrema importância para a proteção dos dados dos usuários de serviços de saúde na medida em que o protocolo auxilia na criação de procedimentos que regulamentam a coleta e compartilhamento dos dados de saúde entre prestadores de saúde e operadoras de planos privados de saúde, e podem reduzir o risco de coleta desnecessária, bem como de compartilhamento indevido de dados. Inclusive, apesar da existência de acordos privados entre os prestadores de serviços de saúde e as operadoras de planos, o Protocolo TISS estabelece as informações que podem ser trocadas no bojo da base legal do "cumprimento de obrigação regulatória" (art. 7º, II; art. 11, II, a), de modo que os dados solicitados fora do padrão devem se enquadrar em outras bases e devem atender princípios como necessidade, finalidade e adequação.

As informações que são abrangidas pelo Padrão TISS são aquelas trocadas por agentes da Saúde Suplementar, quais sejam[8]: i) troca dos dados de atenção à saúde, gerados na modalidade reembolso das despesas assistenciais ao beneficiário de plano privado de assistência à saúde, no

[8] O Padrão TISS não abrange os dados referentes aos eventos de atenção à saúde oriundos de ressarcimento ao Sistema Único de Saúde (Padrão TISS – Componente Organizacional. Outubro/2020).

envio de informação das operadoras de planos privados de assistência à saúde para a ANS; ii) 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 da operadora de planos privados de assistência à saúde.

Outras medidas de proteção ao fluxo de informações relativas à assistência prestada aos beneficiários de planos de saúde privados estão previstas na Resolução Normativa nº 255, de 18 de maio de 2011, e na Resolução Normativa nº 389, de 26 de novembro de 2015. Tais resoluções versam, respectivamente, sobre a designação de Responsável pela Área Técnica da Saúde, que deve zelar pelo fluxo de informações relativas à assistência prestada aos beneficiários; e sobre disponibilização de conteúdo mínimo de informações referentes aos planos de saúde para garantir a transparência das informações no âmbito da saúde suplementar.

Ademais, em relação à proteção das informações dos beneficiários, destaca-se a Súmula Normativa nº 27, de 10 de junho de 2015, que veda a não concretização de proposta de contratação de plano de saúde com base em seleção de risco. Ou seja, as operadoras de saúde não podem negar a cobertura de usuários com base em informações dos usuários que possibilitem a realização de perfilamento, vedação que também está prevista na LGPD, no art. 11, § 5º[9]. Tal medida é tida como um complemento ao art. 14 da Lei nº 9.656, de 3 de junho de 1998, que veda que as operadoras privadas de saúde impeçam o ingresso de

[9] § 5º É 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.

beneficiários em razão da idade ou por serem portadores de deficiência.

5.2. Agência Nacional de Vigilância Sanitária - Anvisa

Outra importante agência que corrobora para a proteção de dados da saúde é a Anvisa. A agência foi criada pela Lei nº 9.782, de 26 de janeiro de 1999, e tem como finalidade promover a proteção da saúde da população, por intermédio do controle sanitário da produção e consumo de produtos e serviços submetidos à vigilância sanitária, inclusive dos ambientes, dos processos, dos insumos e das tecnologias a eles relacionados, bem como o controle de portos, aeroportos, fronteiras e recintos alfandegados (Portal Oficial Anvisa).

Demonstrando a harmonia entre a função regulatória da agência e a proteção de dados, recentemente foi elaborado o Guia nº 38/2020, "*Princípios e práticas de cibersegurança em dispositivos médicos*", que contém o entendimento da Anvisa sobre as melhores práticas em relação a procedimentos, rotinas e métodos considerados adequados ao cumprimento de requisitos técnicos e administrativos exigidos pela agência. Dentre as medidas apontadas, destaca-se a recomendação que fabricantes de dispositivos médicos adotem medidas de proteção de dados, como, por exemplo:

- "*O fabricante deve considerar se os dados relacionados à segurança do paciente são armazenados ou transferidos para/do dispositivo requerem algum nível de proteção, tal como criptografia. Por exemplo, as senhas devem ser armazenadas como hashes criptograficamente seguros*" (pp. 10).
- "*O fabricante deve considerar se são necessárias medidas de controle de risco sobre a confidencialidade para*

proteger os campos de controle/sequenciamento de mensagens nos protocolos de comunicação ou para impedir o comprometimento dos materiais de codificação criptográfica" (pp. 10).

Necessário ressaltar que uma importante função da agência é normatizar, controlar e fiscalizar produtos, substâncias e serviços de interesse para a saúde (art. 2º, III, da Lei nº 9.782/1999). Daí a edição das Resoluções da Diretoria Colegiada nº 9, de 20 de fevereiro de 2015 e nº 10, de 20 de fevereiro de 2015, que tratam, respectivamente, do regulamento para realização de ensaios clínicos com medicamentos e dispositivos médicos no Brasil. Como se verá na Parte II infra., a realização de ensaios clínicos é um importante aspecto sobre o qual a LGPD incide, sendo necessária a confluência dos procedimentos e protocolos dispostos na RDC nº 09/2015 e as garantias aos direitos do titular previstos na LGPD.

5.3. Conselho Federal de Medicina - CFM

O CFM é o órgão de supervisão da ética profissional que atua em conjunto com os Conselhos Regionais para representar os interesses da classe médica, contribuindo para o constante desenvolvimento das boas práticas do setor. Não à toa, o órgão é importante interlocutor na adequação dos procedimentos adotados pelos prestadores de serviços de saúde e na proteção de dados dos pacientes.

A começar pelo Código de Ética Médica, Resolução CFM nº 2.217, de 27 de setembro de 2018, existem diversos dispositivos que versam sobreo tratamento de dados, como, por exemplo, o art. 54 que prevê a necessidade de autorização do paciente ou de seu representante legal quando do compartilhamento de informações entre médicos sobre o quadro clínico do paciente. Além disso, é possível

mencionar os artigos 73 ao 79, que tratam do sigilo profissional, artigo 89 que trata do manuseio de documentos e o artigo 101 que trata da pesquisa médica.

Observe-se que, em relação ao resguardo de tais informações, estão previstas as hipóteses nas quais o consentimento é necessário e quando nem mesmo a autorização do paciente é suficiente para possibilitar a divulgação da informação.

Art.	Ação vedada	Quando a ação é permitida?
73	Revelar fato de que tenha conhecimento em virtude do exercício de sua profissão	Quando houver motivo justo, dever legal ou consentimento, por escrito, do paciente.
74	Revelar sigilo profissional relacionado a paciente criança ou adolescente, desde que estes tenham capacidade de discernimento, inclusive a seus pais ou representantes legais	Quando a não revelação possa acarretar dano ao paciente

75	Fazer referência a casos clínicos identificáveis, exibir pacientes ou imagens que os tornem reconhecíveis em anúncios profissionais ou na divulgação de assuntos médicos em meios de comunicação em geral	Nunca
76	Revelar informações confidenciais obtidas quando do exame médico de trabalhadores, inclusive por exigência dos dirigentes de empresas ou de instituições	Quando o silêncio puser em risco a saúde dos empregados ou da comunidade.
77	Prestar informações a empresas seguradoras sobre as circunstâncias da morte do paciente sob seus cuidados, além das contidas na declaração de óbito	Expresso consentimento do representante legal
89	Liberar cópias do prontuário sob sua guarda	Para atender a ordem judicial ou para sua própria defesa, e quando autorizado por escrito pelo paciente

101	Realizar pesquisa envolvendo seres humanos.	Quando o consentimento for obtido e após as devidas explicações sobre a natureza e as consequências da pesquisa. No caso de o paciente participante de pesquisa ser criança, adolescente, pessoa com transtorno ou doença mental, em situação de diminuição de sua capacidade de discernir, além do consentimento de seu representante legal, é necessário seu assentimento livre e esclarecido na medida de sua compreensão

Em relação aos prontuários dos pacientes, principal fonte de informações sensíveis, além da vedação constante no Código de Ética Médica, destacam-se a Resolução CFM nº 1.605, de 15 de setembro de 2000, que trata da necessidade de consentimento para o compartilhamento de informação do prontuário e ficha médicas; Resolução CFM nº 1.821, de 23 de novembro de 2007, atualizada pela Resolução CFM nº 2.218, de 23 de novembro de 2007, que trata da digitalização e uso de sistemas digitalizados para a guarda e manuseio de prontuários médicos; e Resolução CFM nº 1.638, de 9 de agosto de 2002, que traz a definição de prontuário médico[10] e os indivíduos responsáveis por ele.

[10] Art. 1º - Definir prontuário médico como o 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.

Além das resoluções do CFM, a Lei nº 13.787, de 27 de dezembro de 2018, também trata da digitalização e da utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.

Por fim, outra Resolução importante para a proteção de dados do paciente é a Resolução CFM nº 1.819/2007, que proíbe a colocação do diagnóstico codificado (Classificação Internacional de Doenças - CID) ou tempo de doença no preenchimento das guias da TISS de consulta e solicitação de exames de seguradoras e operadoras de planos de saúde concomitantemente com a identificação do paciente. Por meio dessa vedação, dificulta-se a exposição de um dado sensível do paciente, que é a identificação de informações sobre o seu estado de saúde. A sensibilidade das informações do CID também foi reconhecida na seara trabalhista, que por meio de decisões[11] do TST declararam a nulidade das cláusulas de convenções coletivas de trabalho que preveem a obrigatoriedade de inclusão do código CID nos atestados médicos dos trabalhadores.

[11] AÇÃO ANULATÓRIA. ATESTADO MÉDICO. EXIGÊNCIA DA INSERÇÃO DA CLASSIFICAÇÃO INTERNACIONAL DE DOENÇAS - CID. NULIDADE DE CLÁUSULA DE CONVENÇÃO COLETIVA DE TRABALHO. É nula cláusula constante de convenção coletiva de trabalho que exija a inserção da classificação internacional de doenças (CID) nos atestados médicos apresentados pelos empregados. Tal exigência obriga o trabalhador divulgar informações acerca de seu estado de saúde para exercer seu direito de justificar a ausência ao trabalho por motivo de doença. Essa imposição viola o direito fundamental à intimidade e à privacidade (art. 5º, X, da CF), sobretudo por não existir, no caso, necessidade que decorra da atividade profissional. Sob esses fundamentos, a Seção Especializada em Dissídios Coletivos, por unanimidade, conheceu do recurso ordinário e, no mérito, por maioria, negou-lhe provimento, vencido o Ministro Ives Gandra Martins Filho. TST-RO-268- 11.2014.5.12.0000, SDC, rel. Min. Maria Cristina Irigoyen Peduzzi, 17.8.2015.

6. Conceitos da LGPD

O primeiro passo para a adequação das atividades setoriais à LGPD é a compreensão dos principais conceitos trazidos pela legislação. A partir desses conceitos a lei determina quais dados podem ser tratados, como e em quais hipóteses, quais obrigações estão atreladas a cada um dos agentes envolvidos no tratamento de dados e até mesmo se a LGPD se aplica ao caso em questão ou não. Como já apresentado anteriormente, o setor da saúde possui particularidades que devem ser consideradas na adequação de seus participantes à LGPD.

Por exemplo, além de paciente, a pessoa física que é atendida por estabelecimentos de serviço de saúde também é titular de dados pessoais e, desde sua entrada, por exemplo, em um hospital, ela fornece dados que são tratados ao longo de todas as etapas de atendimento. Assim, para melhor compreensão sobre qual base legal utilizar no tratamento desses dados, é necessário identificar quais dados são tratados, quem são os agentes de tratamento envolvidos e se são dados que se sujeitam a aplicação da LGPD.

O esclarecimento quanto à categorização dos dados e ao conceito de tratamento também importa para a realização da adequação dos procedimentos internos. Isso porque é necessário compreender quais setores tratam dados pessoais e para quais finalidades, antes de analisar o enquadramento da base legal e garantir que o compartilhamento desses dados, os direitos dos titulares e as obrigações dos controladores de dados, estão sendo realizados nos termos previstos pela legislação. Assim, listamos abaixo as características dos principais tipos de dados mencionados pela LGPD, bem como o que é o

"tratamento" a que a legislação se refere e os principais atores envolvidos

Tutela da Saúde

De acordo com o RGPD, trata-se da base legal aplicável 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, se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional.

Dado pessoal é toda informação relacionada a pessoa natural identificada ou identificável.

Por exemplo, endereço, telefone, e-mail, conta corrente, nome dos pais, data de nascimento, RG, CPF

Dado pessoal sensível é o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural

Nos serviços de saúde são considerados dados sensíveis informações sobre doenças, deficiências, riscos de doenças, relatórios médicos, prontuários, resultado de exames, dados biométricos, informações genéticas, dentre outros

Dado de Saúde

Interessante notar que a LGPD não traz o conceito de saúde trazido pela RGPD, fazendo menção tão somente aos conceitos de “Dado Pessoal” e “Dado Pessoal Sensível”, sendo possível a definição do conceito de “Dados de Saúde” a partir da legislação europeia, qual seja: “todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro. Inclui informações sobre a pessoa singular recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação”.

Dado anonimizado é o dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

IMPORTANTE: os dados anonimizados não são objeto de aplicação da LGPD, uma vez que não são relacionáveis ao seu titular

Dado pseudonimizado é o dado relativo ao titular que não possa ser identificado, senão pelo uso de informação adicional.

pseudonimização: tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro

Banco de dados:

conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

Tratamento

Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Ressalta-se que nos serviços de saúde o tratamento de dados pode se dar para duas finalidades distintas: atividade meio ou atividade fim.

Atividade Meio: Utilização de cadastro para marketing; Realização de cobrança de serviços prestados; Recursos humanos; Realização de cadastro de novo paciente com informações básicas (endereço, telefone, e-mail)

Atividade fim: Realização de exames; Análise de prontuário para diagnóstico; Arquivo de histórico do paciente; Compartilhamento de dados entre médicos para realização de tratamento; Pesquisas clínicas

PRINCIPAIS SUJEITOS ENVOLVIDOS NO TRATAMENTO DE DADOS PESSOAIS

ANPD - autoridade nacional

órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional

CONTROLADOR*

pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais

TITULAR

pessoa natural a quem se referem os dados pessoais que são objeto de tratamento

OPERADOR

pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador

ENCARREGADO*

pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD

*** CONTROLADOR e ENCARREGADO** são considerados os **AGENTES DE TRATAMENTO**

!ATENÇÃO!

Os prestadores privados de serviços de saúde devem ter atenção especial com o **PRONTUÁRIO MÉDICO**, tendo em vista que o documento possui uma quantidade substancial e relevante de dados pessoais e sensíveis do paciente, podendo incluir informações de saúde de seus familiares. Tal fato torna indispensável a adoção de medidas técnicas e administrativas voltadas para a proteção de tais informações, pois sua divulgação e compartilhamento indevidos podem resultar em sanções nos termos do art. 52 da LGPD.

Dessa forma, além das obrigações relativas nos art. 11 do Código de Ética Médica (Resolução CFM nº 1.931/2009) quanto ao dever de sigilo do médico em relação as informações confidenciais obtidas no desempenho de suas funções, e art. 1º a Resolução CFM nº 1.605/2000 que prevê a impossibilidade de divulgação do prontuário sem o consentimento do paciente, a LGPD inova ao trazer proteção adicional as informações do paciente.

Para melhor compreensão dos conceitos acima descritos, imagine uma situação na qual uma pessoa vai ao hospital após sentir fortes dores abdominais. Na recepção, o paciente fornece seus **dados pessoais**, informando seu nome, telefone, data de nascimento, CPF, número da carteira do plano de saúde, etc... para realização de seu cadastro e obtenção de autorização do plano de saúde. Já na triagem, o paciente é questionado sobre alguns **dados sensíveis** como informações sobre alergias a medicamentos e histórico de doenças pelo enfermeiro ou médico responsável, que registra tais dados em um prontuário.

Após a triagem, o paciente é encaminhado para um médico que, após avaliação clínica, entende serem necessários exames adicionais para diagnosticar o paciente, pedindo que ele realize alguns exames laboratoriais e de

imagem no próprio hospital, que conta com um laboratório de apoio para análise de determinadas amostras. Utilizando os conceitos acima, observe que nessa situação, o paciente é o **titular dos dados**, e perante ele, o laboratório de apoio e o hospital são **controladores** nas operações de tratamento de dados relativas aos exames laboratoriais. O laboratório, por sua vez, poderá figurar como **operador,** no contrato de prestação de serviços com o hospital relativo às atividades de tratamento de dados para fins de auditoria e prestação de contas, que tem fundamento regulatório.

Ademais, veja-se que entre o registro do paciente na recepção e a consulta médica foram coletados e armazenados diversos **dados pessoais** e **sensíveis**, além de outras informações que serão geradas e posteriormente tratadas quando da realização dos exames adicionais. Dessa situação quotidiana dos prestadores de serviço de saúde diversas outras questões são suscitadas: em quais momentos os dados do paciente (titular) foram tratados ao longo de todos os procedimentos aos quais ele foi submetido? O compartilhamento dos exames entre laboratório e hospital precisam do consentimento do paciente? Quais os direitos do paciente em relação aos seus dados e quais as obrigações do hospital e laboratório? Apesar de não existirem respostas simples para esses apontamentos, essas e outras questões serão analisadas com maior profundidade nos próximos itens.

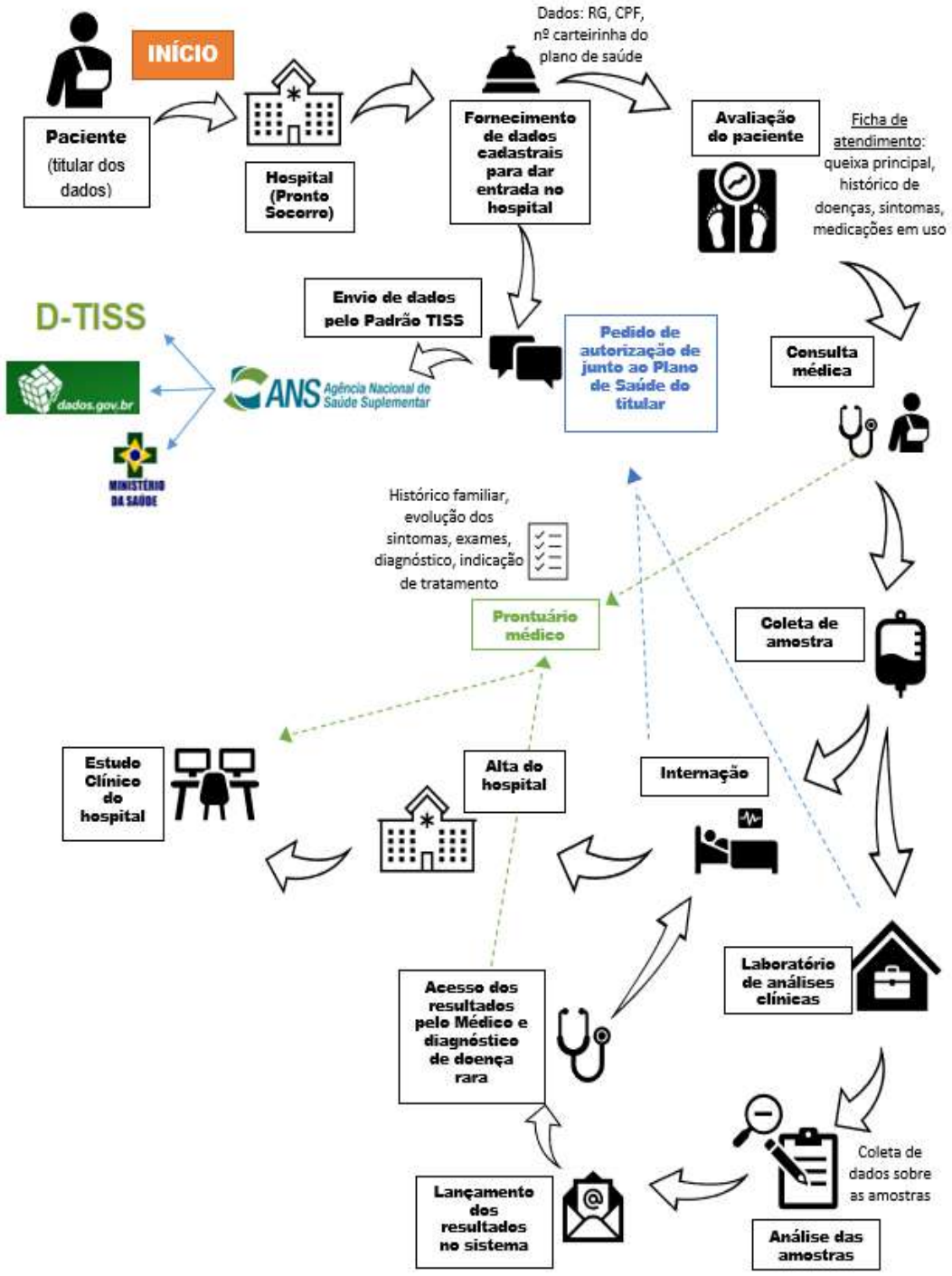
7. Âmbito de aplicação

a. *Prestadores privados de serviço de saúde (Hospitais e SADTs)*

Conforme mencionado, a LGPD dispõe sobre o tratamento de dados pessoais da pessoa natural, ou seja, o objetivo da lei é a proteção dos "direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade" do titular pessoa física dos dados. Ademais, ressalta-se que a lei não se aplica ao tratamento de dados pessoais realizados por pessoa natural para fins exclusivamente particulares e não dotados de proveito econômico e realizados para fins exclusivamente jornalísticos, artísticos, de segurança pública, defesa nacional, segurança de Estado ou atividades de investigação. Em relação a aplicação da lei para fins acadêmicos, este deve se enquadrar nas bases legais previstas no art. 7º e 11º da LGPD.

No caso do setor de saúde, ela se aplica aos dados dos pacientes e profissionais dos estabelecimentos, e não àqueles dados referentes à atividade da empresa. Nesse aspecto, ressalta-se que este guia de boas práticas tem como foco o tratamento de dados realizado pelos prestadores privados de saúde, compreendidos como profissionais de saúde e serviços de saúde. Já os serviços de saúde são aqueles estabelecimentos destinados a promover a saúde do indivíduo, protegê-lo de doenças e agravos, prevenir e limitar os danos a ele causados e reabilitá-lo quando sua capacidade física, psíquica ou social for afetada.

8. Ciclo de vida dos dados no setor de saúde (fluxograma)



PARTE II

1. Protocolo de atendimento

1.1 Aspectos principais

Conforme pode ser observado no Item 8. da Parte I deste Código de Conduta, existem diversos momentos nos quais dados pessoais e dados pessoais sensíveis são tratados (coletados, armazenados, manipulados...) ao longo da passagem dos pacientes pelos estabelecimentos de saúde. Nesse sentido, o Protocolo de atendimento tem como objetivo apresentar os principais momentos nos quais ocorrem o tratamento de dados e os tipos de dados tratados, quais sejam: **a) fornecimento de dados cadastrais na entrada; b) consulta médica e manuseio do prontuário de paciente; c) realização de exames laboratoriais; d) atendimento via telemedicina**.

Veja-se que nas ocasiões acima apontadas são coletados tanto dados sensíveis quanto dados pessoais considerados "ordinários". Por esse motivo, a análise da legalidade do tratamento de dados deverá perpassar necessariamente pela correlação entre o tipo de dado tratado e a finalidade de seu tratamento. Ademais, considerando a existência de diplomas normativos específicos que regulam o setor de saúde, também deve ser levado em consideração as Resoluções do CFM e a Lei nº 13.787/2018, que trazem importantes dispositivos acerca dos dados que são tratados durante o atendimento do paciente.

Vale ressaltar que as principais bases legais utilizadas nos Protocolos de Atendimento são: **a) Art. 7º LGPD - Execução de contrato; b) Art. 7º LGPD - legítimo interesse; c) Art. 7º e 11º LGPD – Consentimento; d) Art. 11 – obrigação regulatória; e) Art. 11 – tutela da saúde; f) Art. 11 – Prevenção à fraude e à segurança do titular; g) Art. 11 – Exercício regular de direito**.

No caso das bases legais aplicáveis aos dados pessoais não sensíveis, a execução contratual seria aplicável aos casos que é necessário utilizar os dados do titular para a realização de cobrança e outros casos nos quais os dados fornecidos sejam necessários para a execução do contrato com o próprio titular. Assim, a base legal é aplicável se o Controlador e o titular tiverem um contrato que tiver que ser executado por meio do processamento ou que alguma condição pré-contratual for necessária para a sua execução.

Quanto ao legítimo interesse, observa-se que esta base legal vincula o tratamento de dados ao escopo das atividades desempenhadas pelo controlador, considerando que a finalidade da operação seja considerada legítima. Tal base legal, embora seja tida como uma das mais flexíveis entre as previstas no art. 7º da LGPD, somente será válida se atender aos critérios legais do art. 7º, IX e art. 10 da Lei. Nesse sentido, o legítimo interesse precisa passar por um triplo teste, que busca avaliar a legitimidade do interesse visado, a necessidade do tratamento de dados e o balanceamento com os direitos do titular.[12] Fundamental é, portanto, que a sua aplicação esteja vinculada aos princípios

[12] O triplo teste está descrito nas orientações da Autoridade do Reino Unido (ICO): https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

da finalidade, necessidade e minimização do uso dos dados, como em alguns casos que o dado do titular é utilizado para o envio de informativos a respeito do controlador dos dados.

Desse modo, para o enquadramento do tratamento de dados à base legal do legítimo interesse, faz-se necessário analisar se o interesse do controlador não se contrapõe a outros comandos legais ou mesmo à liberdade do titular. Por fim, o tratamento deve ser realizado da forma menos invasiva possível, com a adoção de medidas que garantam os direitos dos titulares. Vale lembrar, ademais, que o legítimo interesse não é aplicável ao tratamento dos dados sensíveis e, portanto, não pode ser usado para fundamentar o tratamento de dados de saúde.

A base legal do consentimento, por sua vez, deve seguir com determinados requisitos para que seja considerado válida. Nos termos do art. 5º, XII, o consentimento é a: "*manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada*". O consentimento como base legal deve oferecer uma escolha real,, devendo constar de cláusula destacada das demais cláusulas contratuais (art. 8, par. 1o, LGPD).. Ademais, o controlador deve ter em vista que o titular pode retirar o consentimento quando bem entender.

Necessário apontar que, nos termos do art. 11, II, da LGPD, o tratamento de dados pessoais sensíveis pode ocorrer sem o consentimento apenas quando for **indispensável** para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de

pesquisa; d) exercício regular de direitos,; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, g) garantia da prevenção à fraude e à segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônico. Com exceção do consentimento, em todos os casos de tratamento de dados pessoais sensíveis o tratamento só deve ocorrer se for necessário para as finalidades elencadas no art. 11, II, da LGPD .

No caso da obrigação legal e regulatória (art. 11, LGPD), o processamento é legítimo quando existe previsão legal à qual o controlador está sujeito, como é o caso das obrigações regulatórias previstas pelo Protocolo TISS para o compartilhamento de dados com operadoras de planos de saúde.

Já a tutela de saúde também merece ressalva, tendo em vista que, não obstante todo o setor de saúde atuar indiretamente para o benefício da saúde do paciente, ela somente será aplicável nos "procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária", não podendo ser aplicável a qualquer processamento de dados do setor da saúde.

Nesse sentido, sugere-se a utilização do conceito previsto na legislação europeia, aplicando-se a tutela da saúde apenas 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, se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional.

Por fim, o exercício regular de direito pode considerar que os dados podem ser utilizados para manifestação no âmbito de processos judiciais, administrativos ou arbitrais, ou outras situações que ele seja indispensável para a garantia de um dia.

1.2. Dados cadastrais

a. Introdução

O primeiro momento de coleta de dados pessoais do paciente/titular é realizado logo em sua entrada no sistema de saúde, quando é necessário realizar o seu cadastro no estabelecimento de saúde. Nessa etapa costumam ser solicitados dados como endereço, telefone, e-mail, data de nascimento, RG, CPF, nº da carteirinha do plano de saúde... Com esses dados, realiza-se o registro do paciente no sistema do estabelecimento, que poderá posteriormente ser complementado com dados financeiros e com o prontuário médico.

Assim, o estabelecimento tem o dever de coletar apenas os dados que são estritamente necessários para a finalidade pretendida, de modo a cumprir com o princípio da necessidade e minimização. A depender da finalidade, uma base legal diferente é aplicável, conforme se observará abaixo. Nessa etapa de coleta dos dados cadastrais, em geral, não são coletados os dados de saúde; contudo, tais dados são utilizados para a identificação do paciente e posteriormente essa base pode ser r alimentada com dados sensíveis, de modo que deve ser observado o disposto na Lei nº 13.787/2018, o Código de Ética Médica, a Resolução CFM nº 1.821/2007 no manejo do cadastro dos titulares e tratamento de dados realizados.

Tendo em vista a multiplicidade de possibilidades do processamento de dados cadastrais, serão analisados os seguintes tipos de tratamento: **a) cadastro do paciente no banco de dados do prestador de serviço; b) realização de cobrança pelo setor financeiro do estabelecimento; c) realização de cobrança por empresa terceirizada d) envio de material de marketing; e) pedido de aprovação da consulta ou procedimento para o plano de saúde.**

Veja-se que alguns usos dos dados cadastrais podem envolver tanto dados ordinários, quanto dados sensíveis, de modo que a base legal aplicável a cada hipótese pode ser diferente a depender do contexto.

b. Controlador/operador

Nas hipóteses de tratamento de dados cadastrais apontadas acima, os estabelecimentos de saúde que realizam a coleta primária do dado com o objetivo de utilizá-los para o desenvolvimento de suas atividades serão considerados os controladores dos dados na sua relação jurídica com o paciente. Contudo, é necessário atentar para as especificidades de cada caso e contexto, pois pode ocorrer que determinados prestadores de serviço terceirizados (como um laboratório que presta serviços para um hospital) eventualmente figurem como operador, como por exemplo, nas hipóteses de auditoria e prestação de contas, cujo tratamento de dados tem fundamento regulatório. Para identificar o papel do prestador é necessário identificar **a quem compete as decisões referentes ao tratamento de dados pessoais.**

Dessa forma, a classificação do controlador nas hipóteses acima se dará da seguinte forma:

a) **cadastro do paciente no banco de dados do próprio prestador de serviço** – o prestador de serviços de saúde que coletou os dados poderá ser o controlador,
b) **realização de cobrança pelo setor financeiro do estabelecimento** – o prestador de serviços de saúde que determinou a cobrança do serviço poderá ser o controlador,
c) **realização de cobrança por empresa terceirizada** – o prestador de serviços de saúde que efetuou o serviço cobrado poderá ser o controlador e a empresa terceirizada que atua em nome do estabelecimento o operador,
d) **envio de material de marketing** - o prestador de serviços de saúde ao qual o material de marketing se refere e que determinou a ação de marketing poderá ser o controlador**;**
e) **pedido de aprovação da consulta ou procedimento para o plano de saúde -** o prestador de serviços de saúde que está solicitando a aprovação poderá ser o controlador.

Ressalte-se que a classificação acima apontada deve servir apenas como um indicativo, devendo o prestador de serviços privados de saúde observar a finalidade específica do tratamento de dados e o papel de cada agente envolvido, a depender do contexto do caso sob análise.

c. Base legal

A utilização de dados pessoais de natureza cadastral compreende uma ampla gama de situações, conforme se

pode depreender dos exemplos mencionados. Alguns dos exemplos fazem referência à execução de atos imprescindíveis para a execução do contrato do qual faz parte o titular dos dados, outros entram em atividades secundárias e outros, ainda, podem se referir a tratamentos previstos em legislação.

Assim, é imperativo considerar os qualificantes de cada uma destas situações e seus contextos para a definição da base legal a ser empregada, que poderá variar, por exemplo, da execução de contrato (art. 7º, V), legítimo interesse (art. 7º, IX), consentimento (art. 7º, I e art. 11, I), cumprimento de obrigação legal ou regulatória (art. 7º, II e art. 11, II, a), entre outras que eventualmente possam ser cabíveis.

d. Período de armazenamento/ eliminação

O período de armazenamento deve seguir o princípio da minimização, de modo que os dados devem ser mantidos enquanto forem pertinentes, adequados e limitados aos fins para os quais são processados. Assim, ainda que a lei não estabeleça um período limite para armazenamento dos dados, tão logo os dados armazenados não sejam adequados aos princípios da finalidade e da necessidade previstos no art. 6º, eles devem ser eliminados.

No caso dos dados de saúde, tendo em vista que mesmo os dados pessoais ordinários costumam ser vinculados aos dados de saúde, é necessário que se observe o previsto na Lei nº 13.787/2018 e na Resolução CFM nº 1.821/2007 quanto à digitalização e à utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Assim, os prontuários dos pacientes devem ser preservados por, no mínimo, 20 anos. Importa ressaltar que, caso os dados cadastrais não

se vinculem a um prontuário, tal prazo não se aplica e os dados pessoais devem ser eliminados tão logo o tratamento de dados seja finalizado.

1.3. Prontuário médico e consulta

a. *Introdução*

A segunda etapa do atendimento do paciente envolve o tratamento de dados sensíveis, tendo em vista que a prestação de serviços de saúde como atividade fim necessariamente envolve a coleta de dados de saúde e o seu manuseio. Por esse motivo, essa pode ser considerada a etapa mais sensível do tratamento de dados realizado no atendimento. Tanto o é que o próprio arcabouço regulatório do setor da saúde dispõe sobre o manuseio de dados do prontuário médico, existindo dispositivos a respeito do manuseio do prontuário do paciente na Lei nº 13.787/2018, o Código de Ética Médica, Código de Ética dos Profissionais de Enfermagem e a Resolução CFM nº 1.821/2007.

A Resolução do CFM nº 1638/02 define o prontuário médico em seu art. 1º como "o 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".

Nesse sentido, o conceito de prontuário médico é bastante amplo e abrange todas as informações de saúde, que podem estar em sistemas e documentos dentro das organizações e que servem de insumo para o médico e profissionais de saúde no atendimento ao paciente. Exceções que não se enquadram nesse conceito são as lâminas, que

têm o prazo de 5 anos de armazenamento, conforme Resolução do CFM nº 1472 /97, bem como as amostras de análises clínicas, cujo prazo de armazenamento não está previsto em norma regulamentar.

Assim, é possível observar que os principais pontos de atenção quanto ao tratamento de dados pessoais realizado com o prontuário do paciente já estão descritos nos diplomas supra citados, quais sejam: **a) Acesso e manuseio das informações do prontuário médico por profissionais de saúde envolvidos no tratamento do paciente que são obrigados ao sigilo profissional; b) Acesso e manuseio das informações do prontuário médico por não obrigados ao sigilo profissional; c) Hospedagem dos prontuários por terceiros; d) Utilização do prontuário médico para gerar diagnósticos com auxílio de softwares; e) Acessar informações do prontuário médico por profissional da saúde obrigado ao sigilo profissional em caso de risco de vida.**

b. *Controlador/operador*

Nas hipóteses de tratamento dos dados do prontuário médico apontadas acima, os profissionais de saúde responsáveis pelo atendimento e posterior preenchimento e manuseio do prontuário médico serão considerados os controladores dos dados. Contudo, caso o estabelecimento de saúde seja um prestador de serviço terceirizado (como um prestador de serviço de TI responsável pela gestão dos documentos eletrônicos), ele figurará como operador dos dados. Para identificar o papel do prestador é necessário identificar **a quem compete as decisões referentes ao tratamento de dados pessoais?**

Por exemplo, uma enfermeira ou um enfermeiro que manuseia o prontuário sob orientação do médico que efetivamente é o responsável pelo prontuário e pelo paciente são apenas operadores. Isso porque, ainda que eles manuseiem e preencham o documento, quem detém o poder decisório é o médico, ainda que tanto o/a médico/a quanto o/a enfermeiro/a possuam o dever de sigilo profissional (vide art. 75 do Código de Ética Médico c/c art. 81 do Código de Ética dos Profissionais de Enfermagem).

Já no caso do estabelecimento (pessoa jurídica) no qual o médico trabalha, a análise quanto ao papel exercido depende da relação entre o agente e o poder decisório exercido sob determinado tratamento de dados. No caso do prontuário, é possível considerar o médico responsável pelo paciente e o estabelecimento de saúde como co-controladores, salvo situações excepcionais.

Em relação aos principais tipos de tratamento de dados pessoais que envolvem o prontuário supracitado, a classificação do controlador nas hipóteses acima se dará da seguinte forma: médico e estabelecimento no qual o médico atua podem ser considerados controladores e os/as enfermeiros/as operadores. Quando o tratamento for realizado por terceiros, a análise acerca da posição ocupada depende da finalidade do tratamento, contudo, caso o agente esteja realizando o tratamento por solicitação do médico ou estabelecimento no qual o médico atua tais profissionais/empresas serão considerados operadores.

Ressalte-se que a classificação acima apontada deve servir apenas como um indicativo, devendo o prestador de serviços privados de saúde observar a finalidade específica do tratamento de dados e o papel de cada agente envolvido, a depender do contexto do caso sob análise.

c. *Base legal*

Em relação aos prontuários médicos, tendo em vista que se é composto por dados pessoais sensíveis, é necessário aplicar as bases legais previstas no artigo 11 da LGPD.

Por exemplo, a base legal em caso de "acesso e manuseio das informações do prontuário médico por profissionais de saúde envolvidos no tratamento do paciente que são obrigados ao sigilo profissional"; "utilização do prontuário médico para gerar diagnósticos com auxílio de softwares"; "acessar informações do prontuário médico por profissional da saúde obrigado ao sigilo profissional em caso de risco de vida" pode ser considerada a tutela da saúde. Já o "acesso e manuseio de informações do prontuário médico por profissionais não obrigados ao sigilo profissional" deve ser realizado com o consentimento do usuário ou por obrigação legal ou regulatória.

a. *Período de armazenamento/ eliminação*

O período de armazenamento deve seguir o princípio da minimização, de modo que os dados devem ser mantidos enquanto forem pertinentes, adequados e limitados aos fins para os quais são processados. Assim, ainda que a lei não estabeleça um período limite para armazenamento dos dados, tão logo os dados armazenados não sejam adequados aos princípios da finalidade e da necessidade previstos no art. 6º eles devem ser eliminados.

No caso dos dados de saúde, é necessário que se observe o previsto na Lei nº 13.787/2018 e na Resolução CFM nº 1.821/2007 quanto a digitalização e a utilização de

sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Assim, os prontuários dos pacientes devem ser preservados por, no mínimo, 20 anos e o processo de eliminação deverá resguardar a intimidade do paciente e o sigilo das informações.

b. *Sigilo/segurança da informação*

As medidas de segurança relativas ao prontuário devem ser reforçadas, tendo em vista que se trata de um dos dados mais sensíveis do paciente armazenados pelos prestadores de serviços. Nesse sentido, recomenda-se que sejam implementadas medidas de controle de acesso aos documentos, para garantir que apenas pessoas autorizadas possam acessar as informações. Além disso, sugere-se que sejam adotados sistemas de rastreamento das atividades realizadas com os dados (modificações, cópia, compartilhamento, etc...) e a implementação de um sistema de validação de transferência de arquivos.

1.4. Exame laboratoriais

a. *Introdução*

Os laboratórios de análises clínicas e de imagem, assim como hospitais e clínicas, trabalham primordialmente com dados sensíveis de saúde. Por esse motivo, além dos riscos comuns aos estabelecimentos de saúde vinculados aos dados cadastrais e ao manuseio do prontuário, é necessário destacar algumas especificidades dos principais tipos de tratamento de dados realizados com exames laboratoriais.

Ademais, além de contar com equipe médica e com técnicos de enfermagem, os laboratórios contam com outros profissionais como os Farmacêuticos que atuam nas análises

clínicas e que também possuem o dever de sigilo regulamentado por meio da Resolução do Conselho Federal de Farmácia nº 596/2014

Conforme exposto em detalhes no Protocolo de Compartilhamento, os exames laboratoriais frequentemente são compartilhados com outros prestadores de serviços de saúde. Contudo, além das preocupações já apontadas, os dados gerados pelos laboratórios constituem grandes bancos de dados de saúde que requerem cuidados adicionais.

Além disso, os exames passam por diversas fases que compreendem, principalmente: **a) a coleta das amostras ou das imagens, b) encaminhamento da amostra ou da imagem para o setor responsável pela análise clínica; c) emissão de laudo diagnóstico; d) divulgação do resultado para o paciente; e) armazenamento dos resultados; f) compartilhamento do resultado com o médico responsável** (será abordado no item 2.4 Infra).

b. *Controlador/operador*

Nas hipóteses de tratamento de dados relativos aos exames laboratoriais apontadas acima, os laboratórios que realizaram a coleta primária do dado com o objetivo de utilizá-los para o desenvolvimento de suas atividades serão considerados os controladores dos dados. Contudo, caso o estabelecimento de saúde seja um prestador de serviço terceirizado (como um laboratório que presta serviços para um hospital), ele figurará como operador dos dados. Para identificar o papel do prestador é necessário identificar **a quem compete as decisões referentes ao tratamento de dados pessoais?**

Ressalte-se que a classificação acima apontada deve servir apenas como um indicativo, devendo o prestador de serviços privados de saúde observar a finalidade específica do tratamento de dados e o papel de cada agente envolvido, a depender do contexto do caso sob análise.

c. *Base legal*

Em relação às bases legais dos principais tipos de tratamentos de dados e as principais finalidades dos exames laboratoriais, também é necessário utilizar as bases legais previstas no art. 11.

No caso da "coleta das amostras ou das imagens"; "encaminhamento da amostra ou da imagem para o setor responsável pela análise clínica"; "emissão de laudo diagnóstico"; "divulgação do resultado para o paciente"; "armazenamento dos resultados", quando realizados por profissional de saúde obrigado ao sigilo médico, a base legal aplicável é a tutela da saúde.

a. *Período de armazenamento/ eliminação*

O período de armazenamento deve seguir o princípio da minimização, de modo que os dados devem ser mantidos enquanto forem pertinentes, adequados e limitados aos fins para os quais são processados. Assim, ainda que a lei não estabeleça um período limite para armazenamento dos dados, tão logo os dados armazenados não sejam adequados aos princípios da finalidade e da necessidade previstos no art. 6º eles devem ser eliminados.

No caso dos dados de saúde é necessário que se observe o previsto na Lei nº 13.787/2018 e na Resolução CFM nº 1.821/2007 quanto a digitalização e a utilização de

sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Assim, quando os exames forem anexados ao prontuário dos pacientes eles devem ser preservados por, no mínimo, 20 anos.

1.5. Telemedicina

a. *Introdução*

A Telemedicina possibilita o exercício da medicina à distância, beneficiando pacientes e profissionais da saúde, por meio da utilização da tecnologia da informação e comunicação. De acordo com a "Declaração de Tel Aviv sobre responsabilidades e normas éticas na utilização da Telemedicina", adotada pela 51ª Assembleia Geral da Associação Médica Mundial, em Tel Aviv, Israel, em outubro de 1999[13], os procedimentos mais comuns da telemedicina compreendem as seguintes práticas:

a. **interação entre o médico e o paciente geograficamente isolado ou que se encontre em um meio que não tem acesso a um médico local;**
b. **interação entre o médico e o paciente, na qual se transmite informação médica eletronicamente (pressão arterial, eletrocardiogramas, etc.) ao médico, o que permite vigiar regularmente o estado do paciente;**
c. **interação em que o paciente consulta diretamente o médico, utilizando qualquer**

[13] Disponível em: https://www.wma.net/policies-post/wma-statement-on-accountability-responsibilities-and-ethical-guidelines-in-the-practice-of-telemedicine/

forma de telecomunicação, incluindo a Internet;

d. **interação entre dois médicos: um fisicamente presente com o paciente e outro reconhecido por ser muito competente naquele problema médico.**

Observe-se que as atividades da telemedicina são muito similares às da medicina tradicional, tendo como diferença o fato de o profissional de saúde e o paciente estarem fisicamente distantes. Nesse sentido, as preocupações apontadas nos itens 1.2. e 1.3. supramencionados também se aplicam a esse protocolo.

Sob a perspectiva da proteção de dados pessoais, contudo, esses avanços tecnológicos podem representar um grande desafio para garantir que os dados dos pacientes estejam seguros e que os procedimentos virtuais não exponham dados sensíveis dos titulares. Além disso, o profissional que optar pela utilização da telemedicina deve observar o princípio da qualidade dos dados e da transparência, previstos tanto na "Declaração de Tel Aviv", quanto no art. 6º da LGPD.

Antes da pandemia do coronavírus, a telemedicina era regida pela Resolução nº 1.643/2002 do Conselho Federal de Medicina, que segue em vigor. Essa norma reconhece tal modalidade de atendimento somente para casos emergenciais, ou ainda quando solicitado pelo médico responsável, possibilitando a emissão de laudos à distância e o suporte diagnóstico e terapêutico com a ajuda de recursos tecnológicos.

No contexto da pandemia, a telemedicina passa a se apresentar como uma solução para reforçar a assistência à

saúde. O Ministério da Saúde ampliou, assim, a atuação da saúde à distância e determinou por meio da Portaria nº 467 o uso da telemedicina para atendimentos durante a pandemia, o que inclui atendimento pré-clínico, assistencial, consultas, monitoramento e diagnósticos, na rede privada e na rede pública.

Em abril de 2020 é aprovada a Lei nº 13.989, que autoriza a telemedicina enquanto durar a pandemia e a conceitua como "o exercício da medicina mediado por tecnologias para fins de assistência, pesquisa, prevenção de doenças e lesões e promoção de saúde".

a. *Controlador/operador*

A Telemedicina possui uma relação entre Controlador e Operador similar aos protocolos 1.2. e 1.3., sendo necessária a avaliação de quem é o responsável pelas decisões referentes ao tratamento de dados pessoais nos termos descritos nos protocolos supracitados. Atenção especial deve ser dada à relação entre o médico e ou o estabelecimento de saúde e as empresas de tecnologia que será descrita em detalhes no protocolo de compartilhamento.

b. *Base legal*

Além das bases legais já informadas no bojo dos protocolos 1.2. e 1.3., a telemedicina também requer atenção especial à utilização dos dados coletados durante a consulta para finalidade diversa do atendimento e tratamento do paciente, especialmente no que concerne ao desenvolvimento de novas tecnologias. Tal aspecto será analisado em detalhes no Protocolo de Compartilhamento.

c. *Período de armazenamento/ eliminação*

O período de armazenamento deve seguir o princípio da minimização, de modo que os dados devem ser mantidos enquanto forem pertinentes, adequados e limitados aos fins para os quais são processados. Assim, ainda que a lei não estabeleça um período limite para armazenamento dos dados, tão logo os dados armazenados não sejam adequados aos princípios da finalidade e da necessidade previstos no art. 6º eles devem ser eliminados.

No caso dos dados de saúde é necessário que se observe o previsto na Lei nº 13.787/2018 e na Resolução CFM nº 1.821/2007 quanto a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Assim, os dados constantes no prontuário dos pacientes devem ser preservados por, no mínimo, 20 anos.

d. *Sigilo/segurança da informação*

Assim como no protocolo referente ao tratamento dos dados do prontuário médico, as medidas de segurança relativas aos dados gerados pelas consultas via Telemedicina devem ser reforçadas, tendo em vista que dados sensíveis do paciente armazenados pelos prestadores de serviços. Nesse sentido, recomenda-se que sejam implementadas medidas de controle de acesso aos documentos, para garantir que apenas pessoas autorizadas possam acessar as informações. Além disso, sugere-se que sejam adotados sistemas de rastreamento das atividades realizadas com os dados (modificações, cópia, compartilhamento, etc...) e a implementação de um sistema de validação de transferência de arquivos.

Ademais, considerando a necessidade de conexão com uma rede sem fio para realização das consultas, a utilização

do recurso da telemedicina deve ser acompanhada de cuidados quanto aos riscos cibernéticos externos e internos. Para tanto, recomenda-se a implementação de soluções Secure SD-WAN e utilização de firewall para proteção da conexão. Também é necessário cuidado em relação à possibilidade de roubo de identidade médica, que pode ocorrer por meio da usurpação ou identificação das credenciais de um usuário em um sistema, devendo o sistema de autenticação ser reforçado (como a utilização do método de dois fatores de identificação).

Na telemedicina, é preciso especial cuidado na transmissão de dados. Lidar com dados de saúde que requerem proteção especial requer uma infraestrutura segura que deve impedir o acesso de terceiros. Isso não inclui apenas conexões seguras de internet. Como parte da videochamada ou da consulta com o médico, deve-se assegurar que a conexão telefônica não possa ser grampeada por pessoas não autorizadas. Além disso, ao transmitir resultados de exames ou quadros clínicos ao interessado, deve-se garantir que a pessoa que recebe as informações é realmente o paciente ou o seu representante e, portanto, tem o direito de receber tais informações.

2. Protocolo de Compartilhamento

2.1. Aspectos principais

Um dos principais pontos de atenção quanto à adequação dos processos de tratamento de dados dos prestadores privados de saúde se refere ao compartilhamento de dados. Conforme já abordado anteriormente, o setor de saúde é um setor amplamente regulado, de modo que algumas opções de compartilhamento podem se enquadrar na hipótese legal de "cumprimento de obrigação legal ou regulatória pelo controlador" (art. 7º, II; art. 11, II, a).

Ainda assim, existem diversas hipóteses de compartilhamento de dados pessoais, especialmente dados de saúde, que não estão previstos na legislação específica do setor, sendo necessárias considerações acerca das melhores práticas para o compartilhamento desses dados sensíveis.

Outro aspecto desafiador enfrentado pelo setor de saúde diz respeito às novas tecnologias em saúde e seus modelos de utilização e remuneração. Enquanto, por um lado, a inovação na prestação de serviços de saúde pode ser um importante passo para garantir o acesso aos serviços de saúde para uma parcela maior da população, o desenvolvimento de tais tecnologias demanda uma grande quantidade de dados sensíveis, que gozam de proteção extra por parte da LGPD.

Um aspecto preliminar a ser considerado no tratamento de dados pessoais por profissionais de saúde é que, caso este seja realizado por meio da anonimização dos dados pessoais a LGPD não incidiria, justamente pelo fato de não ocorrer o tratamento de dados pessoais. Nestes casos, é necessário

atentar para a qualidade do processo de anonimização que, caso deixe a desejar, enseja a aplicabilidade da lei. Em regra, portanto, as utilizações que permitirem o uso de dados anonimizados sem prejuízo de sua utilidade devem ser consideradas prioritariamente.

Quanto à base legal, o compartilhamento dos dados depende da categoria dos dados que serão objeto do tratamento, mas a principal base aplicável pode ser o consentimento (art. 7º, I e 11, I) – especialmente para os dados que são compartilhados entre os operadores e os prestadores.

Conforme mencionado anteriormente, a base legal do consentimento deve considerar a presença de determinados requisitos para que seja considerada válida, como previsto no art. 5º, XII, ele deve ser a: "*manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada*".

Assim, em sua aplicação para o tratamento de dados sensíveis e não sensíveis, o consentimento como base legal deve oferecer um escolha real ao titular, sem ser apresentado como uma opção pré-preenchida (*Privacy by Default*), devendo ser oferecida uma forma de escolha efetiva separada dos termos e condições. Ademais, o controlador deve ter em vista que o titular pode retirar o consentimento quando bem entender, devendo fornecer os instrumentos para que possa retirar este consentimento de forma clara e facilitada.

Tendo em vista que a revogação do consentimento pode prejudicar a atividade daqueles que pretendem utilizar os dados de saúde para o desenvolvimento de novas plataformas, modelos de negócio e modelos de

remuneração, é premente que a ANS, o Ministério da Saúde e a ANPD trabalhem em torno da elaboração de padrões e técnicas que devem ser utilizados para o desenvolvimento de novas tecnologias, especialmente as que utilizam dados sensíveis como subsídio, com a finalidade de fornecer maior segurança e legitimidade ao tratamento de dados nestas circunstâncias.

É necessário apontar que, nos termos do art. 11, II, da LGPD, o tratamento de dados pessoais sensíveis pode ocorrer sem o consentimento apenas quando for **indispensável** para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa; d) exercício regular de direitos,; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, g) garantia da prevenção à fraude e à segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônico.

Com exceção do consentimento, em todos os casos de tratamento de dados pessoais sensíveis o tratamento só deve ocorrer se não houver alternativa para que a finalidade almejada seja alcançada, caso contrário, ele não será considerado legítimo. No caso da obrigação legal e regulatória (art. 11, LGPD), o processamento é legítimo quando existe previsão legal à qual o controlador está sujeito, como é o caso das obrigações regulatórias previstas no Protocolo TISS para o compartilhamento de dados com operadoras de planos de saúde.

Já a utilização da base legal da tutela de saúde também merece ressalvas, tendo em vista que, não obstante todo o

setor de saúde atuar indiretamente para o benefício da saúde do paciente, ela somente será aplicável nos "procedimentos realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária", não podendo, portanto, ser aplicável indistintamente para qualquer processamento de dados do setor da saúde.

Nesse sentido, sugere-se a utilização do conceito previsto na legislação europeia, aplicando-se a tutela da saúde apenas 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, se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional.

Por fim, ressalte-se que o recurso à base legal do exercício regular de direito deve considerar que os dados podem ser utilizados para manifestação no âmbito de processos judiciais, administrativos ou arbitrais, ou outras situações que ele seja indispensável para a garantia de um direito, não sendo hábil, portanto, a fornecer a devida fundamentação para outras atividades de tratamento.

2.2. Compartilhamento entre os profissionais de saúde

a. *Introdução*

Sabe-se que, durante o tratamento do paciente, o profissional de saúde por vezes precisa compartilhar informações com colegas da profissão para dirimir dúvidas, obter uma segunda opinião sobre determinado diagnóstico

ou outras finalidades diretamente relacionadas à tutela da saúde do paciente. Tal prática implica no tratamento de dados pessoais sensíveis do titular/paciente, e, portanto, necessita cumprir com os requisitos legais previstos na LGPD.

Tais situações podem nem sempre estar claras para o profissional de saúde, porém são centrais para garantir o cumprimento com a lei. Por exemplo, um clínico geral pode necessitar do auxílio de um neurologista para diagnosticar determinados sintomas, ou quer discutir um caso específico com outro colega da mesma área, e, para isso, circula dados do seu paciente em meios de comunicação. Caso algum dado que permita a identificação do paciente seja divulgado, ou mesmo os exames dele sejam compartilhados, o caso atrai a incidência da LGPD, devendo estar embasado em uma base legal que permita tal compartilhamento.

Além disso, é necessário que sejam atendidos os princípios da boa-fé objetiva, necessidade e finalidade, ainda que o compartilhamento seja feito em prol da saúde do titular. O cuidado com o tratamento realizado deve ser redobrado considerando que as informações compartilhadas são consideradas dados sensíveis e podem expor a intimidade do paciente.

Assim, além da necessidade de cumprimento com o disposto no Código de Ética Médica quanto ao compartilhamento de informações do prontuário, o Conselho Federal de Medicina emitiu o Parecer nº 14/2017 quanto ao uso do WhatsApp e demais plataformas de comunicação entre médicos, em caráter privativo, justamente considerando a ampla utilização desses meios de comunicação entre médicos, chegando à seguinte conclusão:

a) Do ponto de vista jurídico, visando promover uma interpretação sistemática das normas constitucionais, legais e administrativas que regem a medicina brasileira, em especial nos termos do art. 5º, incisos XIII e XIV, da Constituição da República, da lei nº 3.268/1957, do Código de Ética Médica, bem como o inafastável sigilo da relação médico-paciente, cremos que a utilização, no contexto da medicina, dos novos métodos e recursos tecnológicos é medida irreversível e que encontra amparo no atual cenário de evolução das relações humanas, já que, como dito, traz incontáveis benefícios ao mister do profissional médico na busca do melhor diagnóstico e do posterior prognóstico dos pacientes e de suas enfermidade

b) Nesse contexto, o uso do aplicativo "WhatsApp", e outros congêneres, é possível para formação de grupos formados exclusivamente por profissionais médicos, visando realizar discussões de casos médicos que demandem a intervenção das diversas especialidades médicas;

c) Todavia, como tais assuntos são cobertos por sigilo, tais grupos **devem ser formados exclusivamente por médicos devidamente registrados nos Conselhos de Medicina**, caracterizando indevida violação de sigilo a abertura de tais discussões a pessoas que não se enquadrem em tal condição;

d) Por outro lado, com base no art. 75 do Código de Ética Médica as **discussões jamais poderão fazer referência a casos clínicos identificáveis, exibir pacientes ou seus retratos em anúncios profissionais, ou na divulgação de assuntos médicos, em meios de comunicação em geral, mesmo com autorização do paciente**;

e) Registre-se, ainda, que os profissionais médicos que participam de tais grupos são pessoalmente responsáveis pelas informações, opiniões, palavras e mídias que disponibilizem em suas discussões, as quais, certamente, devem se ater aos limites da moral e da ética médica.

Veja-se que o CFM veda que sejam divulgados dados pessoais dos pacientes em grupos formados apenas por médicos, ainda que esses sejam feitos com o consentimento do titular - requisito de natureza ética que, notadamente, amplia a proteção garantida em lei. Ou seja, em consonância com o art. 75 do Código de Ética Médica, o Parecer nº 14/2017 prevê a impossibilidade de se fazer referência a casos clínicos identificáveis, exibir pacientes ou imagens que os tornem reconhecíveis em anúncios profissionais ou na divulgação de assuntos médicos em meios de comunicação em geral.

Ainda que as situações nas quais o médico atua como pessoa física/profissional de saúde ou como representante de um estabelecimento por vezes seja a mesma, é importante diferenciar os dois cenários, tendo em vista que em sua atuação como profissional e saúde ele também está sujeito à aplicação das do disposto no Código de Ética Médica.

O mencionado Parecer coloca, ainda, a cargo dos organizadores do grupo que tomem as devidas providências para que este seja composto somente de médicos com registro no Conselho de Medicina, desautorizando em absoluto, portanto, a divulgação das informações a que faz referência para fora do círculo profissional.

b. *Controlador/operador*

No caso do compartilhamento de dados entre médicos, o médico que recebeu o dado pode ser, a princípio, considerado o operador, quando o médico responsável pelo paciente busca apenas uma segunda opinião. Isso porque a decisão a respeito dos dados compartilhados seria do médico responsável pelos dados de saúde. No entanto, resulta

imperioso considerar as características específicas do tratamento para que se verifique as modalidades de tratamento empregadas pelo médico que recebe o dado - caso nestas se verifique operações que demandem ou impliquem em maior autonomia, ainda mais em se considerando a natureza da atividade médica, não é excluído que este possa ser caracterizado como um controlador conjunto.

Ressalta-se que tal relação independe de o compartilhamento ocasionar em uma infração ao Código de Ética Médica, tendo em vista que este também prevê a impossibilidade de o médico responsável pelo paciente revelar dados que possibilitem sua identificação. Ou seja, a identificação do controlador e do operador, não está estritamente vinculada às particularidades da regulação setorial, podendo assumir outras configurações a depender da finalidade do tratamento realizado.

Assim, conforme mencionado anteriormente, para identificar o papel do prestador é necessário identificar **a quem compete as decisões referentes ao tratamento de dados pessoais.**

Ressalte-se que a classificação acima apontada é um mero indicativo, devendo o prestador de serviços privados de saúde observar a finalidade específica do tratamento de dados e o papel de cada agente envolvido e outros fatores específicos do contexto para que possa determinar a resposta mais adequada para cada situação.

c. *Base legal*

Nos casos nos quais o compartilhamento do dado pessoal é indispensável para a realização de finalidades

legítimas, as bases legais mais frequentemente aplicáveis são, conforme a situação, o consentimento e a tutela da saúde.

Ressalte-se que há um qualificador para a finalidade considerada legítima para o compartilhamento de dados pessoais no setor de saúde: pela LGPD, o tratamento de dados de saúde por meio do compartilhamento, com finalidade econômica, deve ser feito apenas quando (art. 11, § 4º): i) for realizado em benefício dos interesses dos titulares; ii) for estritamente necessário, iii) para prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde.

Ademais, deve ser observado o previsto no Código de Ética Médica, que já prevê situações de compartilhamento de dados de saúde, quais sejam:

- **Revelar fato de que tenha conhecimento em virtude do exercício de sua profissão** - Quando houver motivo justo, dever legal ou consentimento, por escrito, do paciente (art. 73)
- **Revelar sigilo profissional relacionado a paciente, criança ou adolescente, desde que estes tenham capacidade de discernimento, inclusive a seus pais ou representantes legais** - Quando a não revelação possa acarretar dano ao paciente (art. 74)
- **Nunca fazer referência a casos clínicos identificáveis, exibir pacientes ou imagens que os tornem reconhecíveis em anúncios profissionais ou na divulgação de assuntos médicos em meios de comunicação em geral** (art. 75)

Importa ressaltar que o exposto acima é mero indicativo do enquadramento legal, podendo variar a depender das especificidades e do contexto de cada caso.

a. *Período de armazenamento/ eliminação*

O período de armazenamento dos dados pessoais deve considerar prioritariamente o princípio da minimização, de modo que os dados devem ser mantidos enquanto forem pertinentes, adequados e limitados aos fins para os quais são processados. Assim, ainda que a lei não estabeleça um período limite para armazenamento dos dados, tão logo os dados armazenados não sejam adequados aos princípios da finalidade e da necessidade previstos no art. 6º eles devem ser eliminados, podendo eventualmente serem arquivados para fins de cumprimento de finalidade secundária, quando aplicável e legítima.

No caso dos dados de saúde, é necessário que se observe o previsto na Lei nº 13.787/2018 e na Resolução CFM nº 1.821/2007 quanto a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Assim, os prontuários dos pacientes devem ser preservados por, no mínimo, 20 anos e o processo de eliminação deverá resguardar a intimidade do paciente e o sigilo das informações.

2.3. Compartilhamento entre os profissionais de saúde e estabelecimentos de saúde

a. *Introdução*

O compartilhamento entre profissionais de saúde e estabelecimento de saúde refere-se a casos como o compartilhamento de dados de saúde realizado por

laboratórios diretamente com o médico responsável, com o objetivo de facilitar o intercâmbio das informações, em prol do paciente; ou o compartilhamento de prontuários e resultados de exames pelo médico com um hospital, para realização de procedimentos cirúrgicos.

Tais situações diferem do compartilhamento realizado somente entre médicos, pois envolve a troca de informações entre o profissional (pessoa física) e o estabelecimento (pessoa jurídica), tendo como finalidade a realização de procedimentos ou análises em benefício do titular.

Ainda é necessário notar que situações nas quais o médico atue como representante de um estabelecimento podem se assemelhar àquelas nas quais ele atua como profissional de saúde. Contudo, é importante compreender que se trata de um cenário diferente, tendo em vista que em sua atuação como profissional de saúde ele também está sujeito à aplicação do disposto no Código de Ética Médica, ao contrário de quando atue como mero representante de estabelecimento.

b. *Controlador/operador*

Assim, como em todos os outros protocolos, a definição do controlador depende da identificação de qual agente é o responsável pelas decisões referentes ao tratamento de dados pessoais. Tendo em vista que, em diversas situações, o profissional de saúde e o estabelecimento são responsáveis por decisões relevantes referentes aos dados, como é o caso da realização de procedimento cirúrgico, nestes casos poderá ser possível considerar a ambos como controladores conjuntos.

No caso do compartilhamento entre laboratórios e médicos, tendo em vista que os médicos costumam ser os responsáveis pela tomada de decisão relativa ao paciente, aventa-se a hipótese de que que o laboratório seja o operador e o médico o controlador dos dados, quando verificado que, no contexto específico, as decisões caibam ao médico e o laboratório siga procedimentos padronizados em sua atividade.

Ressalte-se que as definições acima apontadas devem servir apenas como um indicativo e a análise dos papéis desempenhados por cada agente depende das especificidades de cada caso.

c. *Base legal*

O compartilhamento de dados entre profissional de saúde e estabelecimentos de saúde deve ser realizado apenas quando estritamente necessário ou quando corresponder a desígnio do titular dos dados pessoais. Para tais casos, a base legal aplicável poderia ser, prioritariamente, o consentimento ou, em casos excepcionais, a tutela da saúde, afora outras situações mais específicas.

Ressalte-se que há um qualificador para a finalidade considerada legítima para o compartilhamento de dados pessoais no setor de saúde: pela LGPD, o tratamento de dados de saúde por meio do compartilhamento, com finalidade econômica, deve ser feito apenas quando (art. 11, § 4º): i) for realizado em benefício dos interesses dos titulares; ii) for estritamente necessário, iii) para prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde.

d. *Período de armazenamento/ eliminação*

O período de armazenamento dos dados pessoais deve seguir prioritariamente o princípio da minimização, de modo que os dados devem ser mantidos enquanto forem pertinentes, adequados e limitados aos fins para os quais são processados. Assim, ainda que a lei não estabeleça um período limite para armazenamento dos dados, tão logo os dados armazenados não sejam adequados aos princípios da finalidade e da necessidade previstos no art. 6º eles devem ser eliminados, podendo eventualmente serem arquivados para fins de cumprimento de finalidade secundária, quando aplicável e legítima.

No caso dos dados de saúde, é necessário que se observe o previsto na Lei nº 13.787/2018 e na Resolução CFM nº 1.821/2007 quanto a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Assim, os prontuários dos pacientes devem ser preservados por, no mínimo, 20 anos e o processo de eliminação deverá resguardar a intimidade do paciente e o sigilo das informações.

2.4. Compartilhamento entre estabelecimentos de saúde

a. *Introdução*

A hipótese de compartilhamento entre estabelecimentos de saúde compreende o compartilhamento de dados entre duas pessoas jurídicas. Por exemplo, quando ocorre a troca de informações sobre o estado de saúde de pacientes entre hospitais, para remanejamento de leitos de UTI.

Ressalte-se que o compartilhamento de dados realizado entre estabelecimentos de saúde e operadoras será descrito em detalhes no item 2.6., de modo que o disposto neste tópico se aplica apenas parcialmente às operadoras.

b. *Controlador / operador*

Assim, como em todos os outros protocolos, a definição do controlador depende da identificação de qual agente é o responsável pelas decisões referentes ao tratamento de dados pessoais. Tendo em vista que os estabelecimentos são responsáveis por decisões referentes aos dados, nestes casos, a depender do contexto específico, é possível considerar ambos como controladores conjuntos.

Ressalte-se que as definições acima apontadas devem servir apenas como um indicativo e a análise dos papéis desempenhados por cada agente depende das especificidades de cada caso.

c. *Base legal*

O compartilhamento de dados entre estabelecimentos de saúde diversos deve ser realizado apenas quando estritamente necessário e no atendimento estrito do princípio da minimização. Nos casos em que o compartilhamento do dado pessoal for indispensável, a base legal aplicável poderá ser, com maior frequência, o consentimento ou, em casos mais específicos, a tutela da saúde, a depender do contexto.

Ressalte-se a existência de qualificador para o tratamento de dados de saúde por meio do compartilhamento com finalidade econômica, que deve ser

feito apenas quando (art. 11, § 4º): i) for realizado em benefício dos interesses dos titulares; ii) for estritamente necessário, iii) para prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde.

d. *Período de armazenamento/ eliminação*

O período de armazenamento deve seguir prioritariamente o princípio da minimização, de modo que os dados devem ser mantidos enquanto forem pertinentes, adequados e limitados aos fins para os quais são processados. Assim, ainda que a lei não estabeleça um período limite para armazenamento dos dados, tão logo os dados armazenados não sejam adequados aos princípios da finalidade e da necessidade previstos no art. 6º eles devem ser eliminados, podendo eventualmente serem arquivados para fins de cumprimento de finalidade secundária, quando aplicável e legítima.

No caso dos dados de saúde, é necessário que se observe o previsto na Lei nº 13.787/2018 e na Resolução CFM nº 1.821/2007 quanto à digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Assim, os prontuários dos pacientes devem ser preservados por, no mínimo, 20 anos e o processo de eliminação deverá resguardar a intimidade do paciente e o sigilo das informações.

2.5. Compartilhamento entre estabelecimentos de saúde e ANS (protocolo TISS)

a. *Introdução*

Conforme mencionado anteriormente, o protocolo TISS, regulamentado pela Resolução Normativa nº

305/2012 da ANS, abrange informações trocadas por agentes da Saúde Suplementar, quais sejam: i) **troca dos dados de atenção à saúde**, gerados na modalidade reembolso das despesas assistenciais ao beneficiário de plano privado de assistência à saúde, no envio de informação das operadoras de planos privados de assistência à saúde para a ANS; ii) **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 da operadora de planos privados de assistência à saúde.

A importância do compartilhamento de dados no bojo dos procedimentos de saúde suplementar é tamanha que a agência publicou a NOTA TÉCNICA Nº 3/2019/GEPIN/DIRAD-DIDES/DIDES (Processo nº 33910.029786/2019-51 da ANS), apresentando os principais tipos de dados tratados pela ANS, quais sejam:

i. cadastros de beneficiários do Sistema de Informações de Beneficiários (SIB);
ii. dados assistenciais da Troca de Informações de Saúde Suplementar;
iii. dados assistenciais dos atendimentos realizados pelo SUS a beneficiários de planos privados de assistência à saúde tratados, bem como as informações e documentos apresentados pelas operadoras na defesa das cobranças dos processos de ressarcimento ao SUS;
iv. informações e documentos utilizados na instrução e defesa em processos administrativos sancionadores por infrações à normas da saúde suplementar;
v. informações e documentos utilizados na instrução e defesa em processos de apuração de fraude em declaração de saúde para fins de rescisão

unilateral de contrato de plano privado de assistência à saúde.

Ademais, de acordo com a Nota Técnica, os operadores de planos privados de assistência à saúde devem enviar à ANS dados relativos aos **cadastros de beneficiários do Sistema de Informações de Beneficiários (SIB) e os dados assistenciais da Troca de Informações de Saúde Suplementar.** No bojo dos processos administrativos da ANS também são trocados dados relativos à cobrança de ressarcimento ao SUS e para apuração de infrações às normas da saúde suplementar; apuração de fraude em declaração de saúde para fins de rescisão unilateral de contrato de plano privado de assistência à saúde.

A ANS vem realizando um trabalho contínuo de adequação dos procedimentos e do seu marco regulatório à LGPD, de modo que algumas das hipóteses previstas neste protocolo podem ser atualizadas ao longo do tempo. Contudo, este protocolo deve servir como apoio para a coordenação dos requisitos legais da LGPD e o marco regulatório do setor de saúde suplementar.

a. *Controlador/operador*

Assim, como em todos os outros protocolos, a definição do controlador depende da identificação de qual agente é o responsável pelas decisões referentes ao tratamento de dados pessoais. Caso se verifique, efetivamente, que tanto ANS como as operadoras são responsáveis pelas decisões referentes aos dados, ambos podem ser considerados controladores conjuntos.

Nos casos de compartilhamento de dados pessoais com estabelecimentos de saúde por exigência regulatória, deve-

se verificar a possibilidade destes serem enquadrados como operadores. Enquanto a ANS e os operadores podem ser considerados co-controladores, hipótese na qual os estabelecimentos não tenham gerência a ponto de tomarem decisões relevantes sobre o uso dos dados. Tal distribuição de papéis considera o cenário no qual a operadora solicita dados para os prestadores de serviços para prestar informações à ANS nos termos do protocolo TISS. Caso informações que não estejam previstas no protocolo TISS sejam solicitadas pelas operadoras, e não sejam exigidas pela ANS, as operadoras podem ser consideradas como únicas controladoras.

Ressalte-se que as definições acima apontadas devem servir apenas como um indicativo e a análise dos papéis desempenhados por cada agente depende das especificidades de cada caso.

b. *Base legal*

A ANS apresenta alguns exemplos do enquadramento dos principais tipos de tratamento nas hipóteses legais na NOTA TÉCNICA Nº 3/2019/GEPIN/DIRAD-DIDES/DIDES (Processo nº 33910.029786/2019-51 da ANS), quais sejam:

BASE LEGAL	TIPO DE TRATAMENTO
Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral **(art. 7º, VI e art. 11, II, "d")**	● Cobrança de ressarcimento ao SUS; ● Apuração de infrações às normas da saúde suplementar; ● Apuração de fraude em declaração de saúde para fins de rescisão unilateral de contrato de plano privado de assistência à saúde.

Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos **(art. 7º, III, e art. 11, II, b)**	● Compartilhamento da Secretaria da Fazenda Nacional com a ANS da base de dados do Cadastro de Pessoas Físicas para fins de enriquecimento e melhoria da qualidade dos dados dos cadastros de beneficiários; ● Compartilhamento do DATASUS com a ANS das bases de dados do Sistema de Informações Hospitalares (SIH) e do Sistema de Informações Ambulatoriais (SAI) para processamento do ressarcimento ao SUS, e do Cartão Nacional de Saúde (CNS), para enriquecimento e melhoria da qualidade dos cadastros de beneficiários; ● Compartilhamento da ANS com o DATASUS do Conjunto Mínimo de Dados (CMD) referentes aos contatos assistenciais na saúde suplementar.
Tutela da saúde, exclusivamente em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária **(art. 7°, VIII e art. 11º, II, "f")**	● Compartilhamento de registros de saúde com os médicos assistentes e outros prestadores de serviços de saúde para melhorar o cuidado e o resultado em saúde para o paciente; ● Utilização de informações de saúde por gestores de sistemas de saúde públicos ou privados para a condução de programas de promoção de saúde e de prevenção de doenças, bem como para o direcionamento dos pacientes para prestadores mais adequados para seus quadros; ● Comunicação à autoridade sanitária de suspeita ou confirmação de doença ou agravo e eventos de saúde pública, como acidentes de trabalho, doenças infecto-contagiosas, violência doméstica, etc; ● Utilização de informações pessoais de saúde pela ANS para subsidiar a formulação de políticas públicas de melhoria do modelo assistencial, bem como para servir de insumo para o monitoramento técnico-assistencial das operadoras, de modo a permitir que a Agência identifique anomalias e intervenha para assegurar a continuidade e a qualidade do cuidado.

a. *Período de armazenamento/ eliminação*

Independentemente da base legal aplicável, o período de armazenamento dos dados pessoais deve seguir o princípio da minimização, de modo que os dados devem ser mantidos enquanto forem pertinentes, adequados e limitados aos fins para os quais são processados. Assim, ainda que a lei não estabeleça um período limite para armazenamento dos dados, tão logo os dados armazenados não sejam adequados aos princípios da finalidade e da necessidade previstos no art. 6º eles devem ser eliminados, podendo eventualmente serem arquivados para fins de cumprimento de finalidade secundária, quando aplicável e legítima.

No caso dos dados de saúde, é necessário que se observe o previsto na Lei nº 13.787/2018 e na Resolução CFM nº 1.821/2007 quanto a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Assim, os prontuários dos pacientes devem ser preservados por, no mínimo, 20 anos e o processo de eliminação deverá resguardar a intimidade do paciente e o sigilo das informações, ainda que esse manuseio seja realizado por órgãos públicos.

2.6. Compartilhamento entre estabelecimentos de saúde e operadoras

Ainda que o compartilhamento entre estabelecimentos de saúde e operadoras de planos de saúde seja em boa medida regulamentado pela ANS por meio das especificações do padrão TISS, existem diversas hipóteses relevantes de compartilhamento de dados entre operadoras e estabelecimentos de saúde que não estão regulamentado ou

não possuem previsões legais passíveis de enquadramento na base legal do "cumprimento de obrigação legal ou regulatória pelo controlador" (art. 7º, II; art. 11, II, a), como o compartilhamento para fins de atendimento primário, coordenação de cuidados ou enriquecimento de dados em plataformas de saúde.

Tendo em vista a relação vertical existente entre operadores e prestadores, por vezes, a relação entre operadores e prestadores privados de saúde podem facilitar o compartilhamento de dados sob pena de descredenciamento, prática considerada abusiva e que pode até mesmo consistir em um ilícito antitruste.

É importante notar, ainda, que a Lei Geral de Proteção de Dados trouxe uma regra especial quanto ao tratamento de dados pessoais sensíveis no seu art. 11, privilegiando o uso do consentimento em detrimento das demais bases legais da lei. Isto porque o legislador, ciente da importância e da criticidade deste tipo de informações, privilegiou a transparência e a informação ao titular dos dados em relação ao uso dos seus dados.

Portanto, ao realizar o tratamento de dados pessoais sensíveis, os agentes de tratamento devem privilegiar a obtenção do consentimento (quando não for a hipótese de dever regulatório acima exposto), oportunizando o paciente a ciência quanto ao uso dos seus dados. O uso de outras bases legais, conforme observado o inciso II do art. 11 é via de exceção e os agentes de tratamento deverão comprovar a indispensabilidade do tratamento, que deverá tomar por base os princípios da lei e o interesse do paciente.

Recomenda-se ainda que o compartilhamento de dados com as operadoras de saúde seja precedido pela obrigação

contratual da coleta de informações respeitando estritamente o princípio da minimização e da vedação do seu uso para outra finalidade:

BOAS PRÁTICAS	
Operadores de serviços de saúde	**Prestadores de serviços de saúde**
- Buscar o consentimento dos paciente para requerer o compartilhamento de dados de saúde (quando não for base legal de cumprimento regulatório), esclarecendo a finalidade e aplicando a minimização de dados; - Requerer somente os dados estritamente necessários para a finalidade necessária, aplicando medidas mitigatórias na integração destes dados; - Retenção dos dados pelo período necessário; - Adotar medidas de segurança da informação	- Compartilhar os dados somente dos pacientes que consentiram ou que o prestador conseguiu capturar o consentimento; - Aplicar medidas mitigatórias para integração de dados - Adotar medidas de segurança da informação

2.6.1. Auditoria

a. *Introdução*

O processo de auditoria interna é uma importante ferramenta de gestão de riscos e controle dos processos internos das operadoras de saúde. Nesse sentido, é

necessário distinguir os processos de auditoria regulares (contábil, operacional, etc...) da auditoria médica, regulamentada pela Resolução CFM nº 1.614/2001, que efetivamente acessa dados de saúde dos pacientes.

Neste tópico tratamos exclusivamente da auditoria médica, que é a realizada pelas operadoras de planos de saúde para verificação dos procedimentos autorizados e para a certificação da adequação dos serviços médicos prestados. Considerando que a realização do procedimento seja necessária para o desempenho das atividades da operadora, devem ser tomados os cuidados necessários relativos à proteção dos dados pessoais da saúde, além de ser necessário o cumprimento do disposto na Resolução CFM nº 1.614/2001.

Nos processos de auditoria são compartilhados dados como cadastro do médico e do paciente, dados do prontuário, detalhes sobre os procedimentos realizados, entre outros. Esse processo pode ser realizado presencialmente porém, por vezes, são realizadas trocas de informações através de meios de comunicação capazes de originarem risco, como por exemplo e-mail. Ou então, podem ser utilizadas práticas com potencial de expor dados pessoais e possibilitar acessos indevidos por profissionais não autorizados.

Nesse sentido, ressalta-se o disposto na Resolução CFM nº 1.614/2001, que prevê diversas obrigações ao médico auditor como, por exemplo, a manutenção do sigilo profissional, sendo vedada a divulgação das observações, conclusões ou recomendações obtidas na auditoria; a comunicação de irregularidades na prestação de serviços e a apresentação do médico responsável ao diretor técnico da unidade auditada. Por outro lado, é vedado ao médico a

aplicação de medidas punitivas ao médico assistente ou à instituição; a intermediação de acordos e a retirada de prontuários ou cópias da instituição.

Esse último aspecto leva a crer que o procedimento de auditoria deve ser realizado, ao menos preferencialmente, *in loco*, ou então que o eventual compartilhamento das informações dos pacientes, caso estritamente necessário, seja realizado por meios eletrônicos seguros.

b. *Controlador/operador*

Assim, como em todos os outros protocolos, a definição do controlador depende da identificação de qual agente é o responsável pelas decisões referentes ao tratamento de dados pessoais. Conforme se observará no item. 2.6.3, a definição do controlador e do operador depende do modelo de remuneração, seja no modelo "*fee for service*" ou em um novo modelo de remuneração.

Considerando que a maioria dos modelos de remuneração na saúde suplementar se estruturam no modelo "*fee for service*", em geral, os operadores de serviços de saúde podem ser, em diversas hipóteses e conforme o contexto, considerados os controladores dos dados, e os prestadores de serviços de saúde os operadores de dados nos contratos de credenciamento.

Quando se tratar dos novos modelos de remuneração, via de regra haverá necessidade de maior trânsito de fluxo de dados, pois tanto os operadores de serviços de saúde quanto os prestadores de serviços de saúde necessitarão de dados para tomar decisões quanto ao paciente. Neste contexto, a figura dos agentes de tratamento dos prestadores de serviços de saúde poderá ser alterada em

relação ao modelo de remuneração de "fee for service" e há maior possibilidade de que, concretamente, ambos os prestadores podem ser considerados controladores conjuntos.

Ressalte-se que a classificação acima apontada deve servir apenas como um indicativo, devendo o prestador de serviços privados de saúde observar a finalidade específica do tratamento de dados e o papel de cada agente envolvido, a depender do contexto do caso sob análise.

c. *Base legal*

Tendo em vista que o compartilhamento de dados entre operadoras e estabelecimentos de saúde para fins de auditoria envolve o tratamento de dados de saúde, a base legal aplicável ao compartilhamento de informações realizado no bojo das auditorias não pode ser definida ampla e livremente pelas partes por meio de contrato. Nesse sentido, recomenda-se que seja coletado o consentimento do paciente para a realização do procedimento ou, quando a realização da auditoria estiver prevista em lei, seja utilizada a base legal "cumprimento de obrigação legal ou regulatória pelo controlador" (art. 7º, II; art. 11, II, a).

Ressalte-se que o tratamento de dados de saúde por meio do compartilhamento com finalidade econômica deve ser feito apenas quando (art. 11, § 4º): i) for realizado em benefício dos interesses dos titulares; ii) for estritamente necessário, iii) para prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde.

d. *Período de armazenamento/ eliminação*

O período de armazenamento deve seguir o princípio da minimização, de modo que os dados devem ser mantidos enquanto forem pertinentes, adequados e limitados aos fins para os quais são processados. Assim, ainda que a lei não estabeleça um período limite para armazenamento dos dados, tão logo os dados armazenados não sejam adequados aos princípios da finalidade e da necessidade previstos no art. 6º eles devem ser eliminados, podendo eventualmente serem arquivados para fins de cumprimento de finalidade secundária, quando aplicável e legítima..

No caso dos dados de saúde, é necessário que se observe o previsto na Lei nº 13.787/2018 e na Resolução CFM nº 1.821/2007 quanto a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Assim, os prontuários dos pacientes devem ser preservados por, no mínimo, 20 anos e o processo de eliminação deverá resguardar a intimidade do paciente e o sigilo das informações.

2.6.2 Atendimento clínico e atenção primária à saúde

a. *Introdução*

Especialmente no que diz respeito à atenção primária à saúde, tanto as prestadoras de serviços de saúde quanto as operadoras buscam otimizar ao máximo os seus processos, tendo em vista que o caráter fundamental desta atividade para o atendimento clínico. As práticas de atenção primária envolvem a coordenação de cuidado, a prevenção das doenças, entre outras nas quais se verifica crescente utilização de tecnologia de informação em saúde. Dessa forma, os estudos sobre a otimização da atenção primária

também acabam envolvendo a relação entre a melhoria da qualidade do cuidado da saúde e incentivos financeiros, para evitar distorções[14].

Tal hipótese já foi em parte abordada no Protocolo 2.5, em relação ao compartilhamento entre estabelecimentos de saúde e a ANS (protocolo TISS), porém existem outras modalidades de compartilhamento de dados além das necessárias para "cumprimento de obrigação legal ou regulatória pelo controlador" (art. 7º, II; art. 11, II, a) na ótica do protocolo TISS.

Por exemplo, o desenvolvimento de estratégias como a disponibilização de dados de prontuário do paciente para utilização pelo profissional de saúde no momento do atendimento, ao mesmo tempo em que pode proporcionar um melhor atendimento pelo profissional de saúde, requer, para que seja viável, o compartilhamento de dados do paciente. Tais dados seriam, no caso, necessários para assegurar a oferta dos serviços desta forma para os pacientes.

Contudo, tal processo por vezes pode implicar no compartilhamento de dados de saúde sem o conhecimento do titular ou mesmo para finalidades por ele desconhecidas, sendo necessário estabelecer diretrizes para a sua realização. Primeiramente deve-se buscar o consentimento do paciente, em observância ao disposto no art. 11, inciso I da LGPD, justamente para que dê transparência do uso dos dados e o seu compartilhamento na cadeia.

---

[14] ANS. Guia para Implementação de Modelos de Remuneração baseados em valor. p. 24 - 25 Disponível em: http://www.ans.gov.br/images/stories/Particitacao_da_sociedade/2016_gt_remuneracao/guia_modelos_remuneracao_baseados_valor.pdf

Recomenda-se, para tal, que para o desenvolvimento e implementação de novas tecnologias e metodologias nesta fase se lance mão da chamada privacidade na concepção, ou "privacy by design", que consiste basicamente na consideração dos efeitos para a privacidade e proteção de dados em todas as fases do processo de elaboração e implementação de uma tecnologia ou metodologia. Desta forma, confere-se maior garantia aos aos titulares, ao mesmo tempo em que se torna viável a introdução de inovações proporcionadas pelo tratamento de dados.

São princípios da concepção de sistemas por meio da privacidade na concepção, ou "privacy by design": i) proatividade e não reatividade; prevenção e não reparação; ii) privacidade como padrão; iii) privacidade incorporada ao design; iv) total funcionalidade – resultado positivo, e não soma zero; v) segurança do começo ao final – proteção do ciclo de vida; vi) visibilidade e transparência; vii) respeito pela privacidade do usuário[15].

Mesmo que não seja abordada de forma direta, a importância da adoção da privacidade na concepção, ou "privacy by design" pode ser observada nos arts. 46 e 50 da LGPD, que preveem a adoção de medidas de segurança e de mitigação de riscos.

[15] Tradução livre de: CAVOUKIAN, Ann. **Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices**. Disponível em: http://dataprotection.industries/wp-content/uploads/2017/10/privacy-by-design.pdf

BOAS PRÁTICAS	
Operadores de serviços de saúde	**Prestadores de serviços de saúde**
- Buscar o consentimento dos paciente para requerer o compartilhamento de dados de saúde (quando não for base legal de cumprimento regulatório), esclarecendo a finalidade e aplicando a minimização de dados; - Requerer somente os dados estritamente necessários para a finalidade necessária, aplicando medidas mitigatórias na integração destes dados; - Retenção dos dados pelo período necessário; - Adotar medidas de segurança da informação	- Compartilhar os dados somente dos pacientes que consentiram ou que o prestador conseguiu capturar o consentimento; - Aplicar medidas mitigatórias para integração de dados - Adotar medidas de segurança da informação

b. *Controlador/operador*

Assim, como em todos os outros protocolos, a definição do controlador depende da identificação de qual agente é o responsável pelas decisões referentes ao tratamento de dados pessoais. Conforme se observará no item. 2.6.3, a definição do controlador e do operador depende do modelo de remuneração, seja no modelo "*fee for service*" ou em um novo modelo de remuneração.

Considerando que a maioria dos modelos de remuneração na saúde suplementar se estruturam no modelo "*fee for service*", em geral, os operadores de serviços de saúde podem ser, em diversas hipóteses e conforme o contexto, considerados os controladores dos dados, e os prestadores de serviços de saúde os operadores de dados nos contratos de credenciamento. Quando se tratar dos novos modelos de remuneração ressalta-se a necessidade de verificar com redobrada cautela as características e o contexto do tratamento, dado que há maior possibilidade de que, concretamente, ambos os prestadores podem ser considerados controladores conjuntos.

Ressalte-se que a classificação acima apontada deve servir apenas como um indicativo, devendo o prestador de serviços privados de saúde observar a finalidade específica do tratamento de dados e o papel de cada agente envolvido, a depender do contexto do caso sob análise.

c. *Base legal*

Uma vez que o compartilhamento de dados entre operadoras e estabelecimentos de saúde para o desenvolvimento de estratégia de atendimento envolve o tratamento de dados de saúde e que esse compartilhamento em geral é utilizado para finalidade diversa da que foi informada na coleta do dado e que não estaria necessariamente prevista em outra base legal. Trata-se de situação em que é relevante considerar a plausibilidade da obtenção do consentimento do paciente (titular dos dados) para a realização do procedimento.

Ademais, o tratamento de dados de saúde por meio do compartilhamento com finalidade econômica deve ser feito apenas quando (art. 11, § 4º): i) for realizado em benefício

dos interesses dos titulares; ii) for estritamente necessário, iii) para prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde.

d. *Período de armazenamento/ eliminação*

O período de armazenamento deve seguir prioritariamente o princípio da minimização, de modo que os dados devem ser mantidos enquanto forem pertinentes, adequados e limitados aos fins para os quais são processados. Assim, ainda que a lei não estabeleça um período limite para armazenamento dos dados, tão logo os dados armazenados não sejam adequados aos princípios da finalidade e da necessidade previstos no art. 6º eles devem ser eliminados, podendo eventualmente serem arquivados para fins de cumprimento de finalidade secundária, quando aplicável e legítima..

No caso dos dados de saúde, é necessário que se observe o previsto na Lei nº 13.787/2018 e na Resolução CFM nº 1.821/2007 quanto a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Assim, os prontuários dos pacientes devem ser preservados por, no mínimo, 20 anos e o processo de eliminação deverá resguardar a intimidade do paciente e o sigilo das informações.

2.6.3. Novos modelos de remuneração

a. *Introdução*

Os novos modelos de remuneração ou remuneração baseada em valor é aquela que prioriza a melhoria da atenção à saúde, e, como consequência, a sustentabilidade do sistema. O cuidado do paciente pode ser realizado por

meio do chamado "*fee for service*" ou pelos novos modelos de remuneração. Dada a importância do tema, a ANS publicou guia para implementação de modelos de remuneração baseados em valor[16], no qual constam as seguintes informações sobre cada um dos modelos:

Em linha com o exposto no Protocolo "*2.6.2 Atendimento clínico e atenção primária à saúde"*, o modelo "fee for service", o mais utilizado pelos prestadores, consiste na cobrança por cada um dos serviços realizados, "*[e]ssa forma de remuneração pressupõe a existência de uma tabela com o valor estabelecido para cada procedimento ou item utilizado, onde a remuneração se dá pelo somatório discriminado de cada um desses procedimentos ou itens utilizados*"[17].

No mencionado Guia para Implantação de Modelos de Remuneração da ANS, são citados outros modelos, como o Pagamento por Desempenho, "Captation", Orçamentação, "Diagnosis Related Groupings" ou DRG, Pagamento por diárias hospitalares e o Assalariamento, e, além de trazer informações como implantar os mencionados modelos, a ANS exemplifica o fluxo de dados necessários para implantação dos modelos de remuneração.

Para fins de tratamento de dados, a diferença entre os modelos consiste na quantidade de dados do paciente que deve ser coletada e compartilhada entre os operadores e

---

[16] ANS. Guia para Implementação de Modelos de Remuneração baseados em valor. p. 24 - 25 Disponível em: http://www.ans.gov.br/images/stories/Particitacao_da_sociedade/2016_gt_remuneracao/guia_modelos_remuneracao_baseados_valor.pdf

[17] ANS. Guia para Implementação de Modelos de Remuneração baseados em valor. p. 19. Disponível em: http://www.ans.gov.br/images/stories/Particitacao_da_sociedade/2016_gt_remuneracao/guia_modelos_remuneracao_baseados_valor.pdf

prestadores de serviços de saúde, além da natureza dos dados.

Veja-se que a remuneração pelo modelo "*captation*" implica em uma maior sofisticação do tratamento dos dados do paciente, sendo necessária a utilização de relações de causalidade para determinar o risco envolvido no valor cobrado.

Representação gráfica da cadeia da saúde e relações jurídicas envolvidas

Baseado no gráfico do IESS – Instituto de Estudos de Saúde Suplementar[18], modificado por Walquiria Favero

Assim, a implementação desses novos modelos de remuneração deve ser feita com cautela, especialmente considerando que a LGPD estabelece, além dos pressupostos legais, uma regra geral de não discriminação aplicável aos processos automatizados [19] - que podem eventualmente incidir nas aplicações do modelo do *captation*. Ademais, é

[18] Disponível em https://www.iess.org.br/?p=setor&grupo=Entenda&desktop=true

[19] SCHERTEL, Laura; FUJIMOTO, Mônica, MATTIUZZO, Marcela. Discriminação algorítmica à luz da Lei Geral de Proteção de Dados. In: Bioni et al (Coords.) **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

necessário estabelecer as finalidades do compartilhamento de forma clara e transparente, além de garantir que este seja realizado estritamente em benefício dos interesses do titular, além de ser imperioso um cuidado maior com o princípio da necessidade, não devendo ser compartilhados os dados a não ser em caso de necessidade para a realização de um procedimento.

Recomenda-se, para tal, que para o desenvolvimento e implementação de novas tecnologias e metodologias nesta fase se lance mão da chamada privacidade na concepção, ou "privacy by design", que consiste basicamente na consideração dos efeitos para a privacidade e proteção de dados em todas as fases do processo de elaboração e implementação de uma tecnologia ou metodologia. Desta forma, confere-se maior garantia aos aos titulares, ao mesmo tempo em que se torna viável a introdução de inovações proporcionadas pelo tratamento de dados.

São princípios da concepção de sistemas por meio da privacidade na concepção, ou "privacy by design": i) proatividade e não reatividade; prevenção e não reparação; ii) privacidade como padrão; iii) privacidade incorporada ao design; iv) total funcionalidade – resultado positivo, e não soma zero; v) segurança do começo ao final – proteção do ciclo de vida; vi) visibilidade e transparência; vii) respeito pela privacidade do usuário[20].

Mesmo que não seja abordado de forma direta, a importância da adoção da privacidade na concepção ou "*privacy by design*" também pode ser observada nos arts. 46

[20] Tradução livre de: CAVOUKIAN, Ann. **Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices**. Disponível em: http://dataprotection.industries/wp-content/uploads/2017/10/privacy-by-design.pdf

e 50 da LGPD, que preveem a adoção de medidas de segurança e de mitigação de riscos.

BOAS PRÁTICAS	
Operadores de serviços de saúde	**Prestadores de serviços de saúde**
- Buscar o consentimento dos paciente para requerer o compartilhamento de dados de saúde (quando não for base legal de cumprimento regulatório), esclarecendo a finalidade e aplicando a minimização de dados; - Requerer somente os dados estritamente necessários para a finalidade necessária, aplicando medidas mitigatórias na integração destes dados; - Retenção dos dados pelo período necessário; - Adotar medidas de segurança da informação	- Compartilhar os dados somente dos pacientes que consentiram ou que o prestador conseguiu capturar o consentimento; - Aplicar medidas mitigatórias para integração de dados - Adotar medidas de segurança da informação

b. *Controlador/operador*

Assim como em todos os outros protocolos, a definição do controlador depende da identificação de qual agente é o responsável pelas decisões referentes ao tratamento de dados pessoais. A definição do controlador e do operador depende do modelo de remuneração, seja no modelo "*fee for service*" ou em um novo modelo de remuneração.

Considerando que a maioria dos modelos de remuneração na saúde suplementar se estruturam no modelo "*fee for service*", em geral, os operadores de serviços de saúde podem ser, em diversas hipóteses e conforme o contexto, considerados os controladores dos dados, e os prestadores de serviços de saúde os operadores de dados nos contratos de credenciamento. Quando se tratar dos novos modelos de remuneração ressalta-se a necessidade de verificar com redobrada cautela as características e o contexto do tratamento, dado que há maior possibilidade de que, concretamente, ambos os prestadores podem ser considerados controladores conjuntos.

Ressalte-se que a classificação acima apontada deve servir apenas como um indicativo, devendo o prestador de serviços privados de saúde observar a finalidade específica do tratamento de dados e o papel de cada agente envolvido, a depender do contexto do caso sob análise.

c. *Base legal*

A princípio, o compartilhamento de dados entre operadoras e estabelecimentos de saúde no bojo dos novos modelos de remuneração envolve o tratamento de dados de saúde. Nesse sentido, é relevante considerar a plausibilidade da obtenção do consentimento do paciente (titular dos dados) para a realização do procedimento.

Ressalte-se que o tratamento de dados de saúde por meio do compartilhamento com finalidade econômica deve ser feito apenas quando (art. 11, § 4º): i) for realizado em benefício dos interesses dos titulares; ii) for estritamente necessário, iii) para prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde.

d. *Período de armazenamento/ eliminação*

O período de armazenamento deve seguir o princípio da minimização, de modo que os dados devem ser mantidos enquanto forem pertinentes, adequados e limitados aos fins para os quais são processados. Assim, ainda que a lei não estabeleça um período limite para armazenamento dos dados, tão logo os dados armazenados não sejam adequados aos princípios da finalidade e da necessidade previstos no art. 6º eles devem ser eliminados, podendo eventualmente serem arquivados para fins de cumprimento de finalidade secundária, quando aplicável e legítima.

No caso dos dados de saúde, é necessário que se observe o previsto na Lei nº 13.787/2018 e na Resolução CFM nº 1.821/2007 quanto a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Assim, os prontuários dos pacientes devem ser preservados por, no mínimo, 20 anos e o processo de eliminação deverá resguardar a intimidade do paciente e o sigilo das informações.

2.7. Compartilhamento entre estabelecimentos de saúde e terceiros

a. *Introdução*

Por fim, a última hipótese deste protocolo versa sobre a possibilidade de compartilhamento de dados com terceiros não vinculados aos estabelecimentos de saúde, compreendendo situações como por exemplo: **a) Realização de contratos com empresas de TI para gestão dos dados de pacientes; b) Compartilhar cópias**

do prontuário sob guarda do médico ou do estabelecimento de saúde para atender ordem judicial ou para defesa própria; c) Compartilhar informações do exame médico de trabalhadores, inclusive por exigência dos dirigentes de empresas ou de instituições; d) Enriquecimento de dados em plataforma de saúde, visando uma gestão completa e integrada de dados de saúde das pessoas (que pode contemplar atendimento primário, gestão populacional, marketplace, etc); e) Compartilhar dados para o desenvolvimento de dispositivos médicos, entre várias outras

b. *Controlador/operador*

Assim, como em todos os outros protocolos, a definição do controlador depende da identificação de qual agente é o responsável pelas decisões referentes ao tratamento de dados pessoais. No caso do compartilhamento entre estabelecimentos de saúde e terceiros, sugere-se que a atribuição dos papéis considere os seguintes elementos:

- **Realização de contratos com empresas de TI para gestão dos dados de pacientes** – nesse caso, a depender do contexto e da natureza do trabalho executado pela empresa de TI, é possível que este seja controladora conjunta do estabelecimento de saúde na gestão de dados dos pacientes. Contudo, dependendo da distribuição de papéis, a empresa também pode figurar como operadora;
- **Compartilhar cópias do prontuário sob guarda do médico ou do estabelecimento de saúde para atender ordem judicial ou para defesa própria** – no caso aquele que compartilhar os dados eventualmente poderá ser considerado como operador,

e o receptor das informações o controlador, tendo em vista que a finalidade do compartilhamento será controlada pelo receptor, conforme deverá se verificar no contexto da situação específica;

- **Compartilhar informações do exame médico de trabalhadores, inclusive por exigência dos dirigentes de empresas ou de instituições** – no caso aquele que compartilhar os dados pode ser eventualmente considerado como operador e o receptor das informações como controlador, tendo em vista que a finalidade do compartilhamento será controlada pelo receptor, conforme deverá se verificar no contexto da situação específica;
- **Compartilhamento de dados em plataforma de saúde, visando uma gestão completa e integrada de dados de saúde das pessoas** – nesse caso é provável que a empresa responsável pela gestão da plataforma e os estabelecimentos sejam controladores conjuntos na gestão de dados dos pacientes, caso se verifique a efetiva divisão de elementos de gestão.
- **Compartilhar dados para o desenvolvimento de dispositivos médicos** - nesse caso é capital atentar para o contexto específico, sendo possível que a empresa responsável pelo desenvolvimento dos dispositivos seja controlador conjunta do estabelecimento de saúde na gestão de dados dos pacientes. Contudo, dependendo da distribuição de papéis, tanto o estabelecimento de saúde quanto o desenvolvedor também podem eventualmente figurar como operadores.

Ressalte-se que a classificação acima apontada deve servir apenas como um indicativo, devendo o prestador de serviços privados de saúde observar a finalidade específica

do tratamento de dados e o papel de cada agente envolvido, a depender do contexto do caso sob análise.

a. *Base legal*

Na maioria dos casos de compartilhamento de dados entre prestadores de serviços de saúde e terceiros a base legal recomendada é o consentimento do paciente, tendo em vista que são tratados dados de saúde por agentes que não são profissionais de saúde, serviços de saúde ou autoridade sanitária, não podendo se aplicar as outras hipóteses do art. 11, II, da LGPD. Assim, por exemplo, para o "compartilhamento de dados em plataforma de saúde, visando uma gestão completa e integrada de dados de saúde das pessoas" é necessário o consentimento.

Em outros casos, como "realização de contratos com empresas de TI para gestão dos dados de pacientes" e "compartilhar dados para o desenvolvimento de dispositivos médicos", a depender o contexto é possível aplicar a base legal prevenção à fraude e à segurança do titular (art. 11, g). Quanto a "compartilhar informações do exame médico de trabalhadores, inclusive por exigência dos dirigentes de empresas ou de instituições", de acordo com o Código de Ética Médica, tal dado pode ser revelado apenas quando o silêncio puser em risco a saúde dos empregados ou da comunidade (art. 76).

Ressalte-se que o tratamento de dados de saúde por meio do compartilhamento com finalidade econômica deve ser feito apenas quando (art. 11, § 4º): i) for realizado em benefício dos interesses dos titulares; ii) for estritamente necessário, iii) para prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde.

a. *Privacy by design*

Recomenda-se, para tal, que para o desenvolvimento e implementação de novas tecnologias e metodologias nesta fase se lance mão da chamada privacidade na concepção, ou "privacy by design", cujo conceito já se encontra detalhado acima.

Mesmo que não seja abordado de forma direta, a importância da adoção da privacidade na concepção ou "privacy by design" também pode ser observada nos arts. 46 e 50 da LGPD, que preveem a adoção de medidas de segurança e de mitigação de riscos.

Quanto aos cuidados relativos à segurança da informação que devem ser tomados no desenvolvimento de dispositivos de saúde por fabricantes, recomenda-se que sejam seguidas as seguintes orientações do Guia nº 38 da Anvisa, que contém "Princípios e práticas de cibersegurança em dispositivos médicos"[21], com as seguintes orientações que os fabricantes de dispositivos médicos devem considerar em seus projetos:

Comunicações seguras

- O fabricante deve considerar como o dispositivo faria interface com outros dispositivos ou redes para a avaliação dos riscos apresentados. As interfaces podem incluir conexões com fio e ou sem fio. Exemplos de métodos de interface incluem Wi-Fi, Ethernet, Bluetooth, USB etc

[21] ANVISA. **Guia nº 38 - Princípios e práticas de cibersegurança em dispositivos médicos**. p. 10 – 11. Disponível em: https://www.gov.br/anvisa/pt-br/assuntos/noticias-anvisa/2020/saiba-mais-sobre-ciberseguranca-em-dispositivos-medicos/guia-38.pdf

- O fabricante deve considerar projetar funcionalidades que atendam todas as entradas (não apenas externas) e levar em consideração a comunicação com dispositivos e ambientes que suportam apenas comunicação menos segura (por exemplo, um dispositivo conectado a uma rede doméstica ou a um dispositivo legado).
- O fabricante deve considerar a transferência de dados de e para o dispositivo protegido para impedir o acesso não autorizado, modificação ou reprodução (replay). Por exemplo, os fabricantes devem determinar: como as comunicações entre dispositivos/sistemas se autenticarem entre eles; se a criptografia é necessária; como a reprodução não autorizada de comandos ou dados transmitidos anteriormente será impedida; e se o encerramento de sessões de comunicação após um tempo pré-definido é apropriado.

Proteção de Dados

- O fabricante deve considerar se os dados relacionados à segurança do paciente são armazenados ou transferidos para/do dispositivo que requer algum nível de proteção, tal como criptografia. Por exemplo, as senhas devem ser armazenadas como *hashes* criptograficamente seguros;
- O fabricante deve considerar se são necessárias medidas de controle de risco sobre a confidencialidade para proteger os campos de controle/sequenciamento de mensagens nos protocolos de comunicação ou para impedir o comprometimento dos materiais de codificação criptográfica.

Integridade do Dispositivo

- O fabricante deve avaliar a arquitetura no nível do sistema para determinar se recursos de projeto são necessários para garantir o não repúdio dos dados (por exemplo, suporte a uma função de trilha de auditoria).
- O fabricante deve considerar riscos à integridade do dispositivo, tais como modificações não autorizadas no software do dispositivo.
- O fabricante deve considerar controles, tais como anti-malware para evitar vírus, *spyware*, *ransomware*, e outras formas de código malicioso a ser executado no dispositivo.

Autenticação do Usuário

- O fabricante deve considerar controles de acesso do usuário que validem quem pode usar o dispositivo ou permita a concessão de privilégios a diferentes funções de usuário ou permita o acesso de usuários em caso de emergência. Ademais, as mesmas credenciais não devem ser compartilhadas entre dispositivos e usuários. Exemplos de autenticação ou autorização de acesso incluem senhas, chaves de hardware, biometria ou um sinal de intenção que não pode ser produzido por um outro dispositivo.

Manutenção de software

- O fabricante deve estabelecer e comunicar um processo para implementação e implantação de atualizações periódicas.
- O fabricante deve considerar como operar o software do sistema, o software de terceiros ou como o software

de código aberto será atualizado ou controlado. O fabricante também deve planejar como responder a atualizações de software ou ambientes operacionais desatualizados fora de seu controle (por exemplo, software de dispositivo médico executando em uma versão não segura de um sistema operacional).

- O fabricante deve considerar como o dispositivo será atualizado para protegê-lo contra vulnerabilidades de cibersegurança recém-descobertas. Por exemplo, pode-se considerar se as atualizações exigirão intervenção do usuário ou serão iniciadas pelo dispositivo e como a atualização pode ser validada para garantir que não tenha efeito adverso na segurança do paciente e no desempenho do dispositivo.
- O fabricante deve considerar quais conexões serão necessárias para realizar atualizações e a autenticidade da conexão ou atualização através do uso de assinatura de código ou de outros métodos semelhantes.

Acesso Físico

- O fabricante deve considerar controles para impedir que uma pessoa não autorizada acesse o dispositivo. Por exemplo, os controles podem incluir bloqueios físicos ou restringir fisicamente o acesso às portas, ou não permitir o acesso com um cabo físico sem exigir autenticação.

Confiabilidade e disponibilidade

- O fabricante deve considerar os recursos de projeto que permitirão ao dispositivo detectar, resistir, responder e se recuperar de ataques de cibersegurança, a fim de manter seu desempenho essencial.

a. *Período de armazenamento/ eliminação*

O período de armazenamento deve seguir o princípio da minimização, de modo que os dados devem ser mantidos enquanto forem pertinentes, adequados e limitados aos fins para os quais são processados. Assim, ainda que a lei não estabeleça um período limite para armazenamento dos dados, tão logo os dados armazenados não sejam adequados aos princípios da finalidade e da necessidade previstos no art. 6º eles devem ser eliminados, podendo eventualmente serem arquivados para fins de cumprimento de finalidade secundária, quando aplicável e legítima.

No caso dos dados de saúde, é necessário que se observe o previsto na Lei nº 13.787/2018 e na Resolução CFM nº 1.821/2007 quanto a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Assim, os prontuários dos pacientes devem ser preservados por, no mínimo, 20 anos e o processo de eliminação deverá resguardar a intimidade do paciente e o sigilo das informações.

1. Protocolo de pesquisa clínica

3.1. Aspectos principais

A pesquisa clínica é um processo de investigação científica envolvendo seres humanos que tem como objetivo o desenvolvimento de medicamentos ou tratamentos eficazes contra determinada doença e a identificação de efeitos adversos aos produtos ou procedimentos objeto do estudo.

Dada a necessidade de proteção do paciente e garantia da segurança do estudo, bem como a importância das pesquisas para o desenvolvimento de novos tratamentos, a pesquisa clínica é objeto de regulamentação tanto pela ANVISA quanto pelo Ministério da Saúde regulamentam os procedimentos (Norma Operacional CONEP nº 001/2013, Resolução CNS nº 506/2016, RDC Anvisa nº 9/2015 e RDC Anvisa nº 10/2015, Resolução CNS nº 251/1997) e as melhores práticas (Guia ICH de Boas Práticas Clínicas, E6(R2), Resolução CNS nº 466/2012). Igualmente, o Código de Ética Médica do CFM trata da matéria, prevendo práticas vedadas ao médico que conduz pesquisas clínicas.

Em relação ao Ministério da Saúde, este atua por meio do CNS, através do CONEP, que atua por meio de uma rede de CEPs, que são organizados nas instituições onde se realizam as pesquisas[22]. O CONEP tem como função a análise dos aspectos éticos das pesquisas clínicas realizadas em áreas temáticas especiais que lhe são encaminhadas pelos CEP das instituições. Já os CEPs têm como atribuição a revisão dos protocolos e pesquisas, tendo a função de

[22] CONEP. Atribuições. Disponível em: https://conselho.saude.gov.br/Web_comissoes/conep/aquivos/conep/atribuicoes.html

proteger os direitos dos voluntários que participam das pesquisas.

A atribuição dos órgãos do CNS são complementares à da Anvisa, que também edita normas a respeito da pesquisa clínica, fato que é representativo da importância e sensibilidade das pesquisas clínicas. Assim, resulta justificada a preocupação deste Guia de Boas Práticas a respeito das especificidades dos estudos clínicos no que concerne o tratamento de dados, especialmente considerando que os ensaios utilizam como subsídio dados de saúde dos participantes.

Os dados de saúde podem ser obtidos de diversas formas, além da coleta primária por meio da ficha clínica como, por exemplo, pelo cruzamento de dados de saúde com outros dados e informações que se convertem em dados de saúde, a depender do contexto (como no caso dos dados de localização utilizados para mapear os possíveis vetores na pandemia da Covid-19). No caso da pesquisa clínica, nos estudos científicos podem ser utilizados tanto informações do paciente (como exames, prontuários e dados fornecidos pelo próprio paciente) quanto informações advindas do cruzamento de dados.

Nesse sentido, o tratamento de dados para efeitos de investigação científica pode ser analisado sob duas perspectivas[23]: a) a sua **utilização primária** - investigação sobre dados de saúde que consiste na utilização direta para fins científicos; b) a sua **utilização secundária** - investigação sobre dados de saúde que consiste no

[23] EDPB. Diretrizes 03/2020 sobre o tratamento de dados relativos à saúde para efeitos de investigação científica no contexto do surto de COVID-19. Abr/2020. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-032020-processing-data-concerning-health-purpose_pt

tratamento posterior de dados recolhidos inicialmente para outros fins. Na utilização primária, os pacientes aptos a participar do estudo têm o seu dado coletado diretamente para a utilização no estudo. Na utilização secundária os titulares forneceram ou tiveram seus dados coletados para outros fins e, posteriormente, esses dados são utilizados nos estudos.

Conforme se observará a seguir, essa distinção impacta tanto a definição sobre quais agentes figuram como controlador ou operador quanto a base legal aplicável, de modo que, além de observar o tipo de dado e a finalidade, no caso da pesquisa clínica também é pertinente observar a distinção entre a utilização primária e secundária dos dados pessoais.

Destaca-se que a base legal mais frequentemente utilizada para a realização de pesquisa clínica é o consentimento, devendo este seguir com determinados requisitos cujas especificações encontram-se na regulamentação específica mencionada para a matéria de pesquisa clínica, para que seja considerado válido. Conforme mencionado no Protocolo de Atendimento, deve ser observado o previsto no art. 5º, XII, que define o consentimento como: "*manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada*". No mais, a forma do consentimento já foi delimitada pelas resoluções do CONEP e outras normas específicas.

3.2. Convite para pesquisa

a. *Introdução*

O tratamento de dados para seleção de potenciais candidatos e o convite para participação é o momento que antecede a realização das pesquisas clínicas. Esse tratamento não é isento de dúvidas por parte dos pesquisadores, especialmente em relação à utilização secundária dos dados de saúde, tendo em vista que, em diversas ocasiões, a base de dados utilizada para seleção dos candidatos aptos a participar dos ensaios é pré-existente e eventualmente não tenha sido obtido o consentimento para que fosse realizado o convite.

Ainda que os convites sejam divulgados ao grande público, para que os resultados efetivamente atestem a eficácia de determinado tratamento ou medicamento é necessária a formação em amostragem adequada e representativa do grupo de participantes, até para garantir a qualidade dos dados que serão coletados. Para tanto, uma das formas mais eficazes de seleção é a utilização de bancos de dados pré-existentes (utilização secundária) para a realização do convite para o paciente.

Assim, nem sempre é possível coletar o consentimento dos pacientes que poderiam ser beneficiados pelos estudos (considere-se igualmente que diversos bancos de dados foram formados antes da entrada em vigor da LGPD) e, ainda que a busca do referido consentimento fosse priorizada, haveria dificuldade considerável em obter amostragem e representatividade ideais para o prosseguimento das pesquisas e a formação dos grupos experimentais no formato mais adequado para que a pesquisa seja exitosa. Ao mesmo tempo, deve-se evitar o tratamento indiscriminado

de dados pessoais e, especialmente, dados pessoais sensíveis de saúde, que podem ser considerados uma violação frontal à LGPD, sendo passível de punição.

Necessário pontuar ainda que, dependendo do objeto de pesquisa, existem requisitos específicos para redução de riscos colaterais para os pacientes alvo e que tais requisitos podem reduzir significativamente o número de pacientes elegíveis para os estudos. Caso tais requisitos não sejam atendidos, é possível que o próprio CEP/CONEP rejeite o protocolo de pesquisa submetido, tendo em vista que as pesquisas clínicas devem ser apreciadas por meio do CEP/CONEP para avaliação ética.

Assim, esse protocolo será dedicado às principais questões atinentes ao tratamento de dados para fins de pesquisas clínicas, tendo em vista a necessidade da sua promoção e, ao mesmo tempo, de que sigam as melhores práticas para a proteção dos dados pessoais dos participantes.

b. *Controlador/operador*

No caso da utilização de bancos de dados para envio dos convites, a identificação do controlador depende do propósito para o qual o dado será utilizado e de quem é o agente responsável pelo tratamento. É possível que o estabelecimento que possua o banco de dados também realize a pesquisa clínica, não havendo dúvidas que ele seja o controlador no tratamento de dados relativos ao convite. Também é possível que médicos diferentes sejam responsáveis pelo paciente que consta no banco de dados ou mesmo que o banco de dados utilizado seja de outra empresa do mesmo grupo. Nesse caso, os dois agentes

podem ser considerados controladores conjuntos, tendo em vista que o banco servirá para propósitos diferentes.

A identificação do propósito para o qual o dado foi coletado (utilização primária ou secundária) impacta na determinação do controlador, pois, aquele que coleta o dado para fins de pesquisa clínica, ainda que seja indiretamente, se torna o controlador desse dado no que diz respeito à pesquisa clínica. Ainda, a depender do contexto, pode haver também algum controlador conjunto que não participe necessariamente do estudo mas que ainda assim figure como controlador no que diz respeito ao tratamento, por exemplo[24].

Por outro lado, o prestador de serviços privados de saúde também pode optar pela contratação de estudos clínicos de uma Organização Representativa de Pesquisa Clínica (ORPC), que ficará encarregada por todas ou por parte das funções relativas ao ensaio. Assim, caso o estudo seja conduzido pela ORPC, incluindo o convite, e o patrocinador (aquele que contratou o estudo) não participe da etapa de seleção, o controlador dos dados é a ORPC e não o prestador.

c. *Base legal*

No tratamento de dados relativos ao convite para pesquisa clínica, confirme aludido, a utilização prioritária da base legal do consentimento é capaz de suprir as demandas em relação à sua legitimidade. Contudo, tendo em vista a existência de bancos de dados pré-existentes, a pertinência

[24] Ver: https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/what-law-says/data-controllers-and-personal-data-health-and-care-research-context/ Acesso em: 12/02/2021

da realização de amostragens a partir de bases de dados de volume considerável e a necessidade de transição para a implementação da LGPD, pode-se vislumbrar igualmente, em cada contexto, a viabilidade da utilização da base legal da tutela da saúde.

Ressalte-se que, para a utilização da base legal da tutela da saúde, o fato do paciente obter benefícios diretos à sua saúde com o estudo é um importante fundamento para a sua legitimidade. Ademais, conforme mencionado anteriormente, o tratamento dos dados para fins de tutela da saúde deve ser realizado por profissionais de saúde, de serviços da saúde ou autoridade sanitária, devendo estes guardar sigilo sobre as informações obtidas no exercício profissional.

Necessário ressaltar a predominância da autonomia do paciente sobre qualquer outra circunstância: assim, mesmo com a utilização da base legal da tutela da saúde, caso o titular demonstre não ter interesse nos contatos a respeito da pesquisa, é necessário que seus dados sejam excluídos do banco de dados para que ele não seja contactado novamente.

Em relação ao consentimento, especialmente em relação ao convite para pesquisa, é necessário observar que este seja informado e concedido livremente. Assim, é necessário assegurar que o titular não se sinta pressionado a participar do estudo ou que seja penalizado de qualquer forma caso não participe. Ademais, caso o consentimento seja fornecido, ainda assim deve-se possibilitar que este seja revogado a qualquer momento e que as operações de tratamento em curso sejam interrompidas.

3.3. Pesquisa Clínica com dados pessoais

a. *Introdução*

O Protocolo de Pesquisa Clínica com Dados Pessoais versa sobre o segundo momento da pesquisa, no qual os dados são coletados e utilizados para realização da pesquisa, principalmente por sua utilização primária. Durante a realização da do estudo, podem ser coletados dados relativos à saúde ou realizados questionários sobre outros dados que podem ser posteriormente correlacionados, bem como podem ser coletados dados ao longo do estudo, como dados relativos à reação do paciente aos medicamentos testados.

Conforme mencionado, a realização da pesquisa possui regulamentação tanto junto à ANVISA quanto ao Ministério da Saúde, que regulamentam estes procedimentos (Norma Operacional CONEP nº 001/2013, Resolução CNS nº 506/2016, RDC Anvisa nº 9/2015 e RDC Anvisa nº 10/2015, Resolução CNS nº 251/1997) e as melhores práticas (Guia ICH de Boas Práticas Clínicas, E6(R2), Resolução CNS nº 466/2012), de modo que o próprio consentimento e o sigilo das informações já foram abordados pelos dispositivos.

Além disso, o "Manual de Orientação: Pendências Frequentes em Protocolos de Pesquisa Clínica" [25] do CONEP/CNS/MS apresenta requisitos específicos sobre como apresentar os detalhes do protocolo pesquisa e até mesmo acerca da redação do Termo de Consentimento Livre e

[25] Disponível em: https://conselho.saude.gov.br/Web_comissoes/conep/aquivos/documentos/MANUAL_ORIENTACAO_PENDENCIAS_FREQUENTES_PROTOCOLOS_PESQUISA_CLINICA_V1.pdf

Esclarecido (TCLE), auxiliando no cumprimento dos princípios da transparência e do consentimento como manifestação livre, informada e inequívoca do titular.

Essa recomendação é reforçada pelo previsto na regulamentação específica da prática por meio da Norma Operacional CONEP nº 001/2013, Resolução CNS nº 506/2016, Resolução CNS nº 251/1997, Resolução CNS nº 466/2012, RDC Anvisa nº 9/2015 e RDC Anvisa nº 10/2015, que tratam da necessidade de se apresentar o TCLE aos participantes das pesquisas, bem como dos procedimentos relativos ao sigilo do estudo.

b. *Controlador/operador*

Assim como descrito no item anterior, a identificação do controlador depende do propósito para o qual o dado será utilizado e de quem é o agente responsável pelo tratamento. É possível que o estabelecimento que possua o banco de dados também realize a pesquisa clínica, podendo então este ser o controlador no tratamento de dados relativo ao Protocolo de Pesquisa. Também é possível que um médico seja responsável pelo paciente que consta no banco de dados seja diferente do pesquisador responsável pelo Protocolo de Pesquisa ou mesmo que o banco de dados utilizado seja de outra empresa do mesmo grupo. Nesses casos, os agentes podem ser considerados controladores conjuntos, tendo em vista que o banco servirá para propósitos diferentes.

Repise-se que a identificação do propósito para o qual o dado foi coletado (utilização primária ou secundária) impacta na determinação do controlador, pois, aquele que coleta o dado para fins de pesquisa clínica, ainda que seja indiretamente, se torna o controlador desse dado no que diz respeito à pesquisa clínica. Ainda, a depender do contexto,

pode haver também algum controlador conjunto que não participe necessariamente do estudo mas que ainda assim figure como controlador no que diz respeito ao tratamento, por exemplo[26].

Caso o prestador de serviços privados de saúde opte pela contratação de estudos clínicos de uma ORPC, é necessária atenção especial aos termos do acordo realizado e a forma de atribuição das funções relativas ao ensaio clínico. A depender dos termos e do contexto do tratamento, o patrocinador e a ORCP podem ser controladores conjuntos ou, caso a ORCP não detenha o controle do tratamento dos dados coletados e tratados, o patrocinador pode eventualmente figurar como controlador e a organização como operadora.

c. *Base legal*

Conforme mencionado anteriormente, a base legal aplicável à Pesquisa Científica é o consentimento. Nesse sentido, recomenda-se a formulação do TCLE nos termos sugeridos pela Norma Operacional CONEP nº 001/2013, qual seja:

> O TCLE apresentado deve conter consentimento de autorização para a coleta, o depósito, o armazenamento e a utilização do material biológico humano atrelado ao projeto de pesquisa específico (Resolução CNS 441/11, itens 2.II e 6; Portaria MS 2.201/11, Capítulo II, Artigos 5° e Capítulo III, Artigo 8). O mesmo TCLE deve ainda informar ao participante a possibilidade de utilização futura da amostra armazenada. Ressalta-se que o uso da

[26] Ver: https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/what-law-says/data-controllers-and-personal-data-health-and-care-research-context/ Acesso em: 12/02/2021

> mesma estará condicionado à: (a) apresentação de novo projeto de pesquisa para ser analisado e aprovado pelo Sistema CEP/CONEP e (b) obrigatoriamente, ao reconsentimento do participante de pesquisa por meio de um TCLE específico referente ao novo projeto de pesquisa (Resolução CNS 441/11, item 6 e Portaria MS 2.201/11, capítulo II, artigo 5 e capítulo IV, seção II, artigos 17, 18 e 22)

d. *Período de armazenamento/ eliminação*

Quando utilizado o consentimento como base legal, é necessário eliminar os dados do titular que porventura revogue o seu consentimento. Ademais, assim como nos outros protocolos, o período de armazenamento deve seguir o princípio da minimização, de modo que os dados devem ser mantidos enquanto forem pertinentes, adequados e limitados aos fins para os quais são processados. Assim, ainda que a lei não estabeleça um período limite para armazenamento dos dados, tão logo os dados armazenados não sejam adequados aos princípios da finalidade e da necessidade previstos no art. 6º eles devem ser eliminados, podendo eventualmente serem arquivados para fins de cumprimento de finalidade secundária, quando aplicável e legítima.

Especialmente no caso da pesquisa clínica, recomenda-se que os participantes sejam informados acerca da possibilidade de tratamento posterior, se for necessário, e que este não seja incompatível com as finalidades iniciais. Ademais, é necessário que se proceda à minimização dos dados por meio da obrigação de especificação dos objetivos e questões investigadas, além da avaliação inicial acerca do

tipo e do volume de dados que serão necessários para que as questões sejam respondidas[27].

e. *Sigilo/segurança da informação*

Além do previsto na LGPD, o tratamento de dados para pesquisa clínica possui um robusto arcabouço regulatório que regulamenta as diversas facetas do tratamento de dados sensíveis. Contudo, é necessário ressaltar medidas de segurança que podem conferir proteção adicional aos dados tratados.

Nesse sentido, ressalta-se a importância da utilização da pseudonimização, em conjunto com outras práticas de segurança, para tornar menos factível a identificação dos titulares dos dados, visto que os seus elementos nominativos não irão sempre acompanhar os dados pseudonimizados em seu tratamento [28] . Veja-se que, diferentemente da anonimização – que o dado pessoal se torna não identificável por conta da desassociação completa – o dado pseudonimizado pode ser associado novamente ao titular. Assim, para que a pseudonimização seja eficaz, deve-se garantir que os dados que permitem a identificação do titular sejam armazenados em locais com acesso controlado para que logrem proporcionar maior segurança.

---

[27] EDPB. Diretrizes 03/2020 sobre o tratamento de dados relativos à saúde para efeitos de investigação científica no contexto do surto de COVID-19. Abr/2020. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-032020-processing-data-concerning-health-purpose_pt

[28] FIOCRUZ. Marcos Legais Pesquisa em saúde. Disponível em: https://portal.fiocruz.br/marcos-legais#:~:text=Para%20entender%20a%20incid%C3%AAncia%20das,direitos%20autorais%E2%80%9D%2C%20abordando%20quest%C3%B5es%20como Acesso em: 12/02/2021.

Assim, sugere-se a realização do processo de encriptação, a assinatura de acordos de não divulgação, além da limitação do acesso aos dados e da manutenção de registro dos acessos realizados aos bancos de dados.

4. Protocolo para exercício dos direitos dos titulares

Conforme especificado no item 2.3. da Parte I supra, a LGPD assegura procedimentos que visam garantir a proteção dos direitos dos titulares e o seu exercício, entre os quais estão os chamados direitos "ARCO" (MENDES, 2019): Acesso; Retificação; Cancelamento e Oposição. Assim, neste protocolo serão apresentadas sugestões para garantia de tais direitos, com base nas melhores práticas internacionais [29]. Veja-se que a garantia do direito dos titulares se vincula às obrigações atribuídas pela LGPD aos controladores dos dados pessoais, como a necessidade de nomeação de um encarregado que receba as reclamações dos titulares, nem como se comunique com a autoridade de proteção de dados e garanta que os procedimentos internos estejam em estrito cumprimento com a legislação de proteção de dados brasileira (art. 41 da LGPD).

[29] Ver: AEPD. Código tipo de la unió catalana d'hospitals. 2020. Disponível em: https://www.aepd.es/sites/default/files/2020-01/ct-uch-cat.pdf; FARMAINDÚSTRIA. Codigo tipo de farmaindustria de proteccion de datos personales en el ambito de la investigacion clinica y de la farmacovigilancia. Nov/2009; ANEIMO; AEDEMO. Codigo de Conducta para el tratamiento de datos de caráter personal por organiaciones de investigación de mercado, social, de la opinión y del análisis de datos. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ ; https://www.hse.ie/eng/gdpr/gdpr-faq/hse-gdpr-faqs-public.pdf.

4.1. Acesso

É direito do titular acessar e receber uma cópia de seus dados pessoais, bem como outras informações que sejam pertinentes ao tratamento de seus dados. Tal pedido pode ser realizado de forma verbal ou escrita e não é possível cobrança de nenhuma natureza para o exercício desse direito, sob pena de impedimento indireto de acesso. Ademais, é necessário estabelecer tempo razoável para resposta dos pedidos, dentro do limite máximo de 15 dias previsto no art. 19, II.

O direito de acesso está diretamente relacionado ao princípio do livre acesso, transparência e prestação de contas, descrito no item 2.1. da Parte I supra, de modo que a recusa em prestar as informações solicitadas deve ocorrer tão somente em situações fundamentadas. Dessa forma, recomenda-se que algumas medidas sejam tomadas pelos prestadores privados de saúde ao preparar o procedimento de atendimento às solicitações de informação, tais como:

- ✓ Estabelecer fluxos para quando for solicitado o direito de acesso e meios para identificar um pedido de informação;
- ✓ Registrar a data do recebimento do pedido;
- ✓ Ter uma política de registro dos pedidos recebidos e criar um canal eficiente para receber tais pedidos;
- ✓ Estabelecer prazos para atender os pedidos de informação, respeitando o limite de 15 (quinze) dias estabelecido no art. 19 da LGPD e hipóteses de interrupção do prazo quando são necessárias informção informações adionais que adicionais que impeçam o atendimento do pedido;

- ✓ Estabelecer os limites das informações que não podem ser prestadas, identificando quais informações são relativas a segredos comerciais e industriais;
- ✓ Possuir sistemas de gerenciamento de informações eficientes que permitam a identificação e localização das informações;
- ✓ Identificar quando um pedido de informação pode envolver informações de outros titulares;
- ✓ Identificar se os dados solicitados são pertinentes e informar, ao menos: i - finalidade específica do tratamento; ii - forma e duração do tratamento, observados os segredos comercial e industrial; iii - identificação do controlador; iv - informações de contato do controlador; v - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; vi - responsabilidades dos agentes que realizarão o tratamento; vii – direitos do titular especificados no art. 18 da LGPD.

4.2. Retificação

O art. 18, III, LGPD garante o direito de retificação de dados que sejam incorretos, incompletos ou desatualizados, em consonância ao princípio da qualidade dos dados, que garante que os dados dos titulares sejam exatos, claros, relevantes e atualizados. Da mesma forma que o pedido de acesso, o pedido pode ser recusado tão somente em hipóteses excepcionais e deve ser atendido, preferencialmente, em até um mês.

- ✓ Estabelecer quando o direito de retificação se aplica e como identificar um pedido de retificação;
- ✓ Registrar a data do recebimento do pedido;

- ✓ Possuir uma política de registro dos pedidos recebidos e criar um canal eficiente para receber tais pedidos;
- ✓ Estabelecer prazos para atender o pedido de retificação e hipóteses de interrupção do prazo quando são necessárias providências adicionais;
- ✓ Ter sistemas de gerenciamento de informações eficientes que permitam a retificação das informações.

4.3. Cancelamento

O titular dos dados tem o direito de solicitar o cancelamento de operações de tratamento que não cumpram os requisitos legais. Ademais, o titular também tem direito de cancelar dados que foram armazenados de forma indevida ou cujo consentimento foi revogado, quando a base legal do consentimento for aplicável. Nesse sentido, sugere-se os seguintes procedimentos para atendimento dos pedidos de cancelamento das operações:

- ✓ Estabelecer quando o direito de cancelamento se aplica e como identificar um pedido de cancelamento;
- ✓ Registrar a data do recebimento do pedido;
- ✓ Possuir uma política de registro dos pedidos recebidos e criar um canal eficiente para receber tais pedidos;
- ✓ Estabelecer prazos para atender o pedido de retificação e hipóteses de interrupção do prazo quando são necessárias providências adicionais;
- ✓ Identificar se foi dado o consentimento para o tratamento do dado e se é possível revogá-lo, de acordo com as normas setoriais;
- ✓ Possuir procedimentos para informar outros operadores que porventura também realizem o tratamento em nome do controlador acerca do cancelamento ou com quem o dado tenha sido compartilhado;

- ✓ Quando o tratamento tiver origem no consentimento do titular ou em contrato, providenciar o acesso do titular à cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento;
- ✓ Fornecer informações claras e adequadas acerca a origem dos dados, a inexistência de registro, os critérios utilizados para o tratamento de dados e a finalidade do tratamento, observados os segredos comercial e industrial ao atender os pedidos do titular;
- ✓ Possuir sistemas de gerenciamento de informações eficientes que permitam o cancelamento das informações e sua eliminação física.

4.4. Oposição

O art. 18, § 2º, da LGPD permite que o titular se oponha a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento aos dispositivos legais. Assim, sugere-se os seguintes procedimentos para o atendimento das solicitações:

- ✓ Identificar a oposição ao tratamento de dados e quando esse direito é aplicável;
- ✓ Registrar a data do recebimento do pedido;
- ✓ Possuir uma política de registro dos pedidos recebidos e criar um canal eficiente para receber tais pedidos;
- ✓ Estabelecer prazos para atender à oposição ao tratamento e hipóteses de interrupção do prazo quando são necessárias providências adicionais;
- ✓ Possuir sistemas de gerenciamento de informações eficientes que permitam a efetivação do direito de

oposição, cancelamento, retificação e outros tipos de alterações relativas aos dados pessoais.

4.5 Modelo de formulário para exercício dos direitos do titular

Para que o exercício dos direitos do titular acima mencionados, sugere-se que um formulário nos moldes apontados abaixo (próxima página) seja disponibilizado para que o titular realize seu pedido.

FORMULÁRIO – SOLICITAÇÃO DE ACESSO, RETIFICAÇÃO, CANCELAMENTO E OPOSIÇÃO DE DADOS PESSOAIS

Nos termos do artigo 9º e 18, da Lei nº 13.709, de 14 de agosto de 2019 (Lei Geral de Proteção de Dados – LGPD), são direitos do titular a I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas em Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos previstos na Lei. Nesse sentido, este formulário tem como objetivo auxiliar o exercício dos direitos do titular dos dados. Caso necessário, solicita-se que seja encaminhada uma cópia deste formulário para outros prestadores de serviços de saúde nos quais você imagine que também exista registro de seus dados.

DADOS DO SOLICITANTE

Nome completo: **Data de nascimento:**

_____ _____

CPF **Nº e plano de saúde** (se aplicável)**:**

_____ _____

Endereço:

_____

Telefone fixo: **Celular**: **E-mail:**

_____ _____ _____

Solicitação:

Acesso
Retificação
Cancelamento
Oposição

1. Por favor, descreva a informação objeto da solicitação:

2. Caso necessário, identifique os documentos que subsidiam seu pedido:

Declaro que as informações apresentadas neste formulário são verdadeiras e que eu sou a pessoa a quem elas se referem, conforme documento de identidade com foto anexado ao pedido.

_____/__ ,__ de _____, ____
CIDADE/UF, DATA

_____
Assinatura

5. Protocolo de Segurança da Informação

O Protocolo de Segurança da Informação tem como objetivo fixar diretrizes gerais que devem ser seguidas pelos prestadores privados de serviço em saúde, nos termos expostos pelo art. 46 da LGPD. Ou seja, os prestadores devem adotar medidas de segurança técnica e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Considerando que o setor de saúde possui grande fluxo de dados sensíveis e, por esse motivo, conta com a proteção adicional de outras normas legais, sendo necessária a confluência de todos os requisitos na elaboração de um sistema de segurança. Assim, recomenda-se que, após a realização do mapeamento do fluxo de tratamento dos dados pessoais, sejam identificados os principais componentes para que as implementações de segurança sejam realizadas de forma mais efetiva. Para tanto, recomenda-se a adoção dos seguintes requisitos[30]:

REQUISITOS DE SEGURANÇA MÍNIMOS

Políticas e Conscientização	Criar, revisar e comunicar diretrizes considerando melhores práticas para assegurar a proteção e privacidade dos dados pessoais.
Gestão de Identidades e Acessos	Fornecer acessos somente as pessoas autorizadas e revogá-los quando a pessoa não trabalhar mais na empresa. Proteger os logins de acesso evitando a exposição desses acessos a pessoas não autorizadas. Adotar um segundo fator de autenticação sempre que possível.

[30] Foram utilizados os controles de segurança especificados no NIST Cyber Security Framework e normativas ISO 27701 /27001.

Gestão de Backups	Garantir que os dados relevantes para o negócio tenham uma cópia de segurança, devidamente protegida contra acessos não autorizados.
Gestão de Ativos	Inventariar os ativos que tratam dados pessoais e garantir os requisitos mínimos de segurança.
Gestão de Segurança Endpoint	Garantir que todos os ativos que tratam dados pessoais tenham uma solução de antimalware instalada e atualizada periodicamente.

REQUISITOS DE SEGURANÇA PRIORITÁRIOS

Monitoramento e Gestão de Incidentes	Monitorar o comportamento dos acessos e da segurança dos ativos envolvidos no tratamento dos dados. Esteja preparado para identificar comportamentos e/ou acessos não autorizados.
Gestão de Fornecedores	Avaliar se o fornecedor contratado que trata dados pessoais possui requisitos mínimos de segurança.
Log de sistemas críticos	Avaliar e garantir que sejam registrados as atividades de tratamentos dos dados: data, horário, duração, identidade do funcionário/responsável pelo acesso e a ação executada/processada.
Controle para Vazamento de Informações	Prevenir o vazamento dos dados pessoais em todo o seu ciclo de tratamento.
Segurança Física	Garantir a segurança do acesso físico às informações tratadas em mídias eletrônica, papel e sistemas.
Gestão de Vulnerabilidade / Pentest	Avaliação a execução de testes de segurança nos sistemas que tratam dados pessoais, priorizando os sistemas expostos na Internet.

REQUISITOS DE SEGURANÇA AVANÇADOS

Arquitetura de Segurança	Analisar e identificar melhorias para a proteção dos dados pessoais envolvendo a arquitetura de tecnologias que suportam os produtos/sistemas.
Transferência de Dados	Garantir a segurança na comunicação durante os processos de transferências de dados.
Exclusão de Dados Tratados	Mapear a localização dos dados pessoais para que possam ser excluídos quando solicitado.
Mascaramento de Dados	Avaliar o uso de mascaramento de dados quando aplicável.
Pseudo-anonimização	Avaliar o uso de pseudo-anonimização quando aplicável.
Desenvolvimento Seguro	Avaliar se o produto/sistema estão integrados na esteira atual que contempla análise e implementação de requisitos de segurança para o desenvolvimento seguro.
Criptografia	Avaliar a aplicação de recursos de criptografia de dados pessoais quando necessária.

Observe-se que tais requisitos representam um cenário ideal de aspectos a serem observados pelos prestadores de serviços de saúde, contudo, é necessário que se considere o estágio de adequação de cada estabelecimento e tipos de sistemas utilizados para tratar dados de saúde na elaboração da estratégia de segurança da informação.

[Código de Boas Práticas]

Proteção de Dados para Prestadores Privados em Saúde

CNSaúde
CONFEDERAÇÃO NACIONAL DE SAÚDE

SRTV/S - Quadra 701, Conjunto E
Ed. Palácio do Rádio I Bloco 3
N° 130 5° Andar Asa Sul Brasília (DF)
CEP 70340-901 **www.cnsaude.org.br**