CÓDIGO DE BOAS PRÁTICAS

Laboratório São Geraldo

Considerações Iniciais

O Laboratório São Geraldo é um estabelecimento de saúde focado em laboratórios de análises clínicas em Varginha/MG. Dada a sua atuação no setor de saúde e o consequente tratamento intensivo de dados pessoais, a atenção aos processos envolvendo o fluxo de informações tornou-se ainda mais valorizada.

Com a entrada em vigor da LGPD, o cuidado com o tratamento de dados e a conscientização dos envolvidos passaram por uma constante evolução, à medida que as tecnologias de informação e comunicação têm criado inovadoras possibilidades no setor.

Para explorar plenamente essas novas oportunidades e consolidar com segurança os processos já implementados que utilizam dados pessoais, é de extrema importância a adaptação ao modelo regulatório introduzido pela Lei Geral de Proteção de Dados (LGPD).

A LGPD reconhece a relevância da informação pessoal nas diversas relações entre o indivíduo e a sociedade, oferecendo ferramentas que contribuem para o controle transparente e eficiente no tratamento de dados, assegurando o uso legítimo desses dados em um ambiente de confiança.

Diante desse novo cenário regulatório, surge a necessidade de adaptação de todas as atividades que envolvem o tratamento de dados pessoais, especialmente no setor de saúde. Além do respeito, sigilo e ética já consagrados nas relações do setor da saúde, o Laboratório São Geraldo busca, mais do que nunca, tratar os dados de forma harmônica, implementando conceitos, princípios e procedimentos que uniformizem o tratamento de dados, gerando uma relação ainda maior de confiança, respeito e credibilidade perante clientes, cooperados e prestadores de serviços.

Assim, o Laboratório São Geraldo concluiu que uma das medidas mais eficazes para se adequar aos marcos normativos de proteção de dados é a criação de normas e procedimentos, materializados em Códigos de Conduta ou de Boas Práticas. Esses códigos buscam aplicar as normas gerais de proteção de dados pessoais a casos específicos de tratamento de dados, incorporando as melhores práticas adotadas. Isso visa sistematizar um conjunto de medidas a serem adotadas pela empresa, comprometendo-se não apenas com o cumprimento da legislação, mas também com a implementação de medidas adicionais e específicas além daquelas prescritas nos documentos normativos.

1. Introdução

A Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/18) foi implementada em setembro de 2020, após 8 anos de intensos debates sobre privacidade e proteção de dados no Brasil. Com a sua aprovação, o país passou a contar com uma legislação moderna e específica sobre o tema, estabelecendo novas regras com o objetivo de proteger a privacidade e intimidade dos indivíduos, por meio da definição de princípios, direitos e deveres para o tratamento de dados pessoais.

A LGPD instituiu a Autoridade Nacional de Proteção de Dados – ANPD, regulamentada pelo Decreto nº 10.474/2020, como o órgão responsável pela supervisão da lei. A ANPD tem a incumbência de elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e Privacidade, além de promover a regulamentação dos setores que lidam com dados pessoais.

Uma das funções da ANPD é coordenar ações com os órgãos e entidades responsáveis por setores específicos da atividade econômica, assegurando seu adequado funcionamento conforme as disposições regulamentares e legislativas.

O início da vigência da LGPD representa um marco significativo para a consolidação dos direitos e garantias fundamentais do indivíduo, com impacto substancial em todos os setores da sociedade. Dada a natureza do setor de saúde, que envolve um considerável fluxo de tratamento de dados pessoais sensíveis, é crucial uma abordagem aprofundada e específica sobre o tema.

Diante desse contexto, e em consonância com a entrada em vigor 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, o Laboratório São Geraldo estabelece seu Código de Boas Práticas, buscando contribuir de maneira efetiva com a implementação da LGPD.

2. 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, este princípio destaca a importância de conduzir o tratamento de dados pessoais de maneira cooperativa e transparente. Envolve agir de forma ética e justa, assegurando que as ações relacionadas ao tratamento de dados possam ser verificadas por meio de atos objetivos, promovendo a confiança entre as partes envolvidas.

II. finalidade: Determina que o tratamento de dados deve ter propósitos legítimos, específicos, explícitos e informados ao titular. Isso significa que a coleta, o processamento e o uso de dados devem ser alinhados com as finalidades para as quais foram inicialmente informados, evitando qualquer utilização posterior incompatível.

III. adequação: este princípio destaca a importância de garantir que o tratamento de dados seja compatível com as finalidades informadas ao titular, levando em consideração o contexto em que os dados são coletados. A adequação refere-se à conformidade com as expectativas razoáveis do titular em relação ao uso de seus dados.

IV. necessidade: Visa a limitação do tratamento ao mínimo necessário para atingir as finalidades informadas. Isso implica a coleta e o uso apenas dos dados essenciais para alcançar os objetivos do tratamento, evitando excessos e garantindo a proporcionalidade.

V. livre acesso: Garante aos titulares o direito de acessar informações sobre o tratamento de seus dados de forma facilitada e gratuita. Essa transparência promove a autonomia do titular, permitindo que este compreenda como seus dados estão sendo utilizados.

VI. qualidade dos dados: Assegura que os dados sejam precisos, claros, relevantes e atualizados, conforme necessário para cumprir a finalidade do tratamento. Esse princípio promove a confiabilidade e a utilidade dos dados.

VII. transparência: Exige que os titulares tenham acesso a informações claras, precisas e facilmente acessíveis sobre o tratamento de seus dados, respeitando os segredos comerciais e industriais. A transparência fortalece a confiança entre as partes envolvidas.

VIII. segurança: Enfatiza a importância de adotar medidas técnicas e administrativas capazes de proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão dos dados que possam comprometer a sua integridade.

IX. prevenção: Orienta para a adoção de medidas proativas a fim de prevenir a ocorrência de danos resultantes do tratamento de dados pessoais. Isso envolve a implementação de práticas preventivas e protocolos de segurança.

X. não discriminação: Proíbe o tratamento de dados para fins discriminatórios ilícitos ou abusivos, reforçando a igualdade e a imparcialidade no tratamento de dados pessoais.

XI. responsabilização e prestação de contas: Exige que os agentes responsáveis pelo tratamento demonstrem, de maneira eficaz, a adoção de medidas que comprovem a conformidade com as normas de proteção de dados pessoais, incluindo a eficácia dessas medidas. Essa responsabilização visa garantir a prestação de contas diante das obrigações legais.

3. Bases legais para o tratamento de dados pessoais

A Lei Geral de Proteção de Dados (LGPD) representa um avanço significativo na proteção das informações pessoais, estabelecendo condições claras de legitimidade para o tratamento de dados pessoais. Conforme estipulado no artigo 7º da LGPD, todo tratamento de dados pessoais deve ter respaldo em uma das bases legais estabelecidas, como consentimento do titular, execução de contrato, proteção da vida, tutela da saúde, legítimo interesse, entre outras.

No contexto específico do setor de saúde, é crucial observar um cuidado adicional, pois a legislação confere proteção especial aos dados considerados sensíveis, incluindo os dados de saúde. Essa proteção é mais abrangente, contemplando um conjunto diferenciado de bases legais para o tratamento dessas informações, conforme previsto no artigo 11 da LGPD.

Além das condições de legitimidade, é imperativo considerar criteriosamente os princípios estabelecidos na LGPD no tratamento de dados. Mesmo quando a base legal utilizada é a "execução de contrato", os dados processados para esse fim devem atender, por exemplo, aos princípios da necessidade e finalidade, conforme estabelecido no artigo 6º, I e III, da LGPD.

Da mesma forma, mesmo quando um dado pessoal é tratado com o consentimento do titular, o tratamento não pode ser conduzido com objetivos discriminatórios, ilícitos ou abusivos, conforme disposto no artigo 6º, IX, da LGPD.

Uma atenção especial é direcionada à base legal da "tutela da saúde", que autoriza o tratamento tanto de dados sensíveis quanto de dados não sensíveis. No entanto, sua aplicação requer cautela, pois o conceito de tutela da saúde não se aplica indiscriminadamente a todas as etapas da prestação de serviços de saúde. Recomenda-se a utilização dessa base legal à luz do conceito de tutela da saúde estabelecido no Regulamento Geral sobre a Proteção de Dados da União Europeia (RGPD).

Os dados pessoais mencionados no artigo podem ser tratados para os fins específicos relacionados à tutela da saúde se estiverem sob a responsabilidade de profissionais sujeitos ao dever de sigilo profissional, conforme estipulado pelo direito da União ou dos Estados-Membros. Portanto, é essencial distinguir quais tratamentos são realizados no escopo das atividades principais dos prestadores de serviços de saúde e por profissionais de saúde sujeitos ao dever de sigilo. Caso contrário, a base legal "tutela da saúde" pode não ser a mais apropriada.

4. Direitos dos titulares

A Lei Geral de Proteção de Dados (LGPD) estabelece procedimentos essenciais para garantir a proteção dos direitos dos titulares e viabilizar o legítimo exercício desses direitos. Os direitos fundamentais conferidos aos titulares, conhecidos pela sigla "ARCO" - acesso, retificação, cancelamento e oposição, são essenciais para o controle do fluxo de seus dados pessoais.

Além da LGPD, outras legislações brasileiras também contemplam direitos do cidadão sobre seus dados. O Código de Defesa do Consumidor (CDC) busca proteger os direitos do consumidor em relação aos seus dados pessoais, especialmente quando presentes em bancos de dados de proteção ao crédito. O Marco Civil da Internet estabelece prerrogativas e direitos aos usuários da Internet em relação aos seus dados. Uma tutela mais abrangente, focada na

proteção de dados pessoais, é observada no Código Civil, a partir da proteção dos direitos de personalidade e da tutela dos direitos subjetivos.

A LGPD, além dos direitos ARCO, introduz outros direitos relevantes para o titular, destacando-se o direito de portabilidade. A portabilidade dos dados pessoais, derivada do poder de controle do titular sobre seus dados, envolve a capacidade do controlador de transferir os dados para outros controladores mediante solicitação do titular. Embora aguarde regulamentação pela Autoridade Nacional de Proteção de Dados (ANPD) para operar, esse direito destaca-se pela sua importância potencial no setor de saúde. Ele oferece ao titular a possibilidade de escolher e alterar controladores conforme sua vontade, o que pode ser relevante ao considerar a mudança de prestadores de serviços de saúde.

5. Agentes do tratamento

Outro ponto importante da LGPD é a introdução da figura dos agentes de tratamento de dados, alinhada com diversos marcos normativos similares, como o Regulamento Geral de Proteção de Dados (RGPD) europeu.

Os agentes de tratamento, que, conforme a LGPD, são o controlador e o operador, são os únicos responsáveis por realizar operações de tratamento de dados, e, de acordo com suas funções, podem ser considerados responsáveis em caso de violação da legislação. Entre as obrigações desses agentes, destaca-se a necessidade de adotar medidas de segurança, técnicas e administrativas, para proteção contra acessos não autorizados. Além disso, é obrigatório registrar as operações de tratamento de dados e elaborar um relatório de impacto.

Obrigações dos agentes de tratamento

Além dos direitos conferidos aos titulares, a LGPD impõe aos agentes de tratamento diversas obrigações durante o processamento de dados pessoais. Isso inclui a obrigação de designar um encarregado de tratamento de dados pessoais (art. 41), manter a segurança da informação

em todos os tratamentos (art. 46 e seguintes) e realizar o registro das operações de tratamento de dados (art. 37).

6. Segurança da informação

A obrigação de garantir a segurança da informação está presente nas diversas obrigações detalhadas nos protocolos da Parte II. É importante destacar que, independentemente da hipótese de tratamento, é fundamental manter os dados em um ambiente controlado e seguro. Recomenda-se, sempre que possível, a utilização de técnicas de anonimização ou pseudonimização dos dados, conforme estabelecido nos artigos 46 e seguintes.

7. Autoridade de garantia e regime sancionatório

Enquanto os dados pessoais proporcionam benefícios sociais, valorização das empresas, serviços públicos mais eficientes e aprimoramento da qualidade do atendimento ao consumidor, é crucial observar que um tratamento inadequado desses dados, sem considerar os princípios e regras da LGPD, pode resultar em responsabilização dos agentes controladores e operadores do tratamento.

As penalidades estabelecidas pelo artigo 52 da LGPD incluem a possibilidade de advertência, aplicação de multas que podem chegar a até 50 milhões de reais, além da suspensão parcial ou total das atividades relacionadas ao 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 ados 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.

8. Boas práticas e governança

Para uma abordagem abrangente do quadro regulatório da proteção de dados no direito brasileiro, é essencial considerar não apenas a LGPD, mas também outras normativas relacionadas, como o Código de Defesa do Consumidor (CDC), o Marco Civil da Internet, a Lei de Acesso à Informação, regulamentações setoriais aplicáveis e outras. Dada a complexidade do tema e a presença de conceitos abertos, a aplicação efetiva da legislação deve ser adaptada aos aspectos individuais dos agentes, levando em conta os riscos e o arcabouço regulatório.

É crucial reconhecer o modelo regulatório híbrido da proteção de dados, utilizando os Códigos de Conduta como meio de coordenar as diversas normativas que incidem sobre um setor ou atividade específica, alinhando-se à lógica e à gramática da LGPD. Essa prática promove a complementaridade entre os instrumentos jurídicos existentes e efetiva a autorregulação prevista no art. 50 da LGPD. No caso do setor de saúde, além do cumprimento dos requisitos

da LGPD, o setor possui sua própria regulação e dinâmica, exigindo uma aplicação que considere essas características.

Portanto, este guia será dividido em duas partes. A primeira parte explorará o marco normativo que conecta a proteção de dados à regulação setorial e analisará o papel das agências regulatórias. Além disso, serão abordados os principais conceitos da LGPD e o âmbito de aplicação do guia, levando em consideração o ciclo de vida típico dos dados no setor.

A segunda parte estabelecerá protocolos para as questões mais sensíveis do setor, como atendimento, compartilhamento, pesquisa clínica, exercício dos direitos dos titulares e segurança da informação.

Cabe destacar que este Guia de Boas Práticas foi elaborado com base no documento da CNSaúde, contando com a colaboração de especialistas em proteção de dados, membros da ANS e representantes do setor de saúde privado. O objetivo é auxiliar a ANPD e outras entidades na aplicação da LGPD no setor, estabelecendo um marco autorregulatório em conformidade com as particularidades normativas da prestação de serviços de saúde, conforme previsto no art. 50 da LGPD.

9. Definições

Agentes de tratamento: Refere-se ao controlador e ao operador, sendo o controlador responsável por determinar as finalidades e meios de tratamento de dados pessoais, e o operador aquele que realiza o tratamento em nome do controlador.

Agência Nacional de Saúde Suplementar (ANS): Órgão autárquico de regulação e fiscalização, atuando em todo o território nacional, responsável por normatizar, controlar e fiscalizar as atividades que garantem a assistência suplementar à saúde.

Autorização prévia de procedimento de saúde: Mecanismo utilizado pelas operadoras para avaliar solicitações de procedimentos de saúde antes de sua realização.

Banco de dados: Conjunto organizado de dados pessoais, podendo estar em suporte eletrônico ou físico, armazenado em um ou mais locais.

Beneficiário: Pessoa que usufrui de um plano privado de assistência à saúde.

Consentimento: Manifestação livre, informada e inequívoca do titular concordando com o tratamento de seus dados pessoais para uma finalidade específica.

Eliminação: Processo de exclusão de dados ou conjunto de dados armazenados em um banco de dados, independentemente do método utilizado.

Internet: Sistema global de comunicação de dados, estruturado por protocolos lógicos, destinado a possibilitar a comunicação entre terminais por meio de diferentes redes, estruturado em escala mundial para uso público e irrestrito.

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.

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: 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: Dispositivo que se conecta à internet, como um computador.

Transferência internacional de dados: Movimento 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.

10. 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 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 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.

11. 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.

12. 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.

13. Ministério da Saúde

- Resolução CNS nº 251, de 07 de agosto de 1997 - Diretrizes e Normas Regulamentadoras de Pesquisa Envolvendo Seres Humanos.

- 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.

14. Regulação setorial

Na prestação de serviços de saúde, existem instituições centrais para a regulação setorial que, mesmo antes da entrada em vigor da LGPD, demonstravam preocupação com a proteção de dados de saúde. Esses órgãos sempre estiveram atentos aos dispositivos normativos que visam salvaguardar os dados dos usuários. Dentre eles, destacam-se a Agência Nacional de Saúde Suplementar – ANS e ii) Agência Nacional de Vigilância Sanitária e Anvisa.

A análise do papel dessas instituições na proteção de dados do usuário e de seus principais dispositivos relacionados ao tema é fundamental para compreender a abordagem setorial em relação à segurança e privacidade das informações de saúde.

15. 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 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:

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 : 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.

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, § 5º8. 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 beneficiários em razão da idade ou por serem portadores de deficiência.

16. Âmbito de Aplicação

Prestadores privados de serviços laboratoriais de análises clínicas

Conforme mencionado, a LGPD regula o tratamento de dados pessoais de pessoas naturais, visando a proteção dos "direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade" dos titulares dos dados. Vale ressaltar que a lei não abrange o tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e sem fins econômicos, bem como para fins exclusivamente jornalísticos, artísticos, de segurança pública, defesa nacional, segurança de Estado ou atividades de investigação.

No que diz respeito à aplicação da lei para fins acadêmicos, é necessário que essa aplicação esteja em conformidade com as bases legais estabelecidas nos artigos 7º e 11º da LGPD. No contexto do setor de saúde, a lei se aplica aos dados de pacientes e profissionais dos estabelecimentos, não se estendendo aos dados relacionados à atividade empresarial.

É importante destacar que este guia de boas práticas se concentra no tratamento de dados realizado pelos prestadores privados de saúde, que englobam profissionais de saúde e serviços de saúde. Os serviços de saúde referem-se aos estabelecimentos destinados a promover a saúde do indivíduo, protegê-lo de doenças, prevenir danos e reabilitá-lo quando sua capacidade física, psíquica ou social for afetada.

PROTOCOLOS DO CÓDIGO DE CONDUTA DE PROTEÇÃO DE DADOS PARA OS PRESTADORES PRIVADOS EM SAÚDE

1. Considerações iniciais

1.1 Aspectos principais

Conforme evidenciado anteriormente, há diversos momentos nos quais dados pessoais e dados pessoais sensíveis são tratados ao longo da jornada dos pacientes nos estabelecimentos de saúde. O Protocolo de Atendimento tem como propósito destacar os principais momentos de tratamento de dados e os tipos de dados tratados, abrangendo: a) fornecimento de dados cadastrais na entrada; b) coleta de materiais; c) realização de exames laboratoriais; d) atendimento à distância; e) entrega de resultados.

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 CFO 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. Fundamental é, portanto, que a sua aplicação esteja vinculada aos princípios 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 considerada 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 odontológicos.

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/odontologia preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico/odontológico, 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 ocorre durante o cadastro no sistema de saúde/laboratorial, geralmente realizado no momento da entrada no estabelecimento. Nessa etapa, são solicitados dados como endereço, telefone, e-mail, data de nascimento, RG, CPF e número da carteirinha do plano de saúde. Esses dados são essenciais para registrar o paciente no sistema do estabelecimento, podendo ser complementados posteriormente com dados financeiros e prontuário odontológico.

O estabelecimento tem a obrigação de coletar apenas os dados estritamente necessários para a finalidade pretendida, cumprindo o princípio da necessidade e minimização. Na fase de coleta de dados cadastrais, em geral, não são coletados dados de saúde; no entanto, esses dados são utilizados para a identificação do paciente, e posteriormente, a base pode ser alimentada com dados sensíveis.

Nessa etapa, diversos tipos de tratamento podem ser realizados com os dados cadastrais, como:

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.

Alguns usos dos dados cadastrais podem envolver tanto dados ordinários quanto dados sensíveis. A base legal aplicável a cada hipótese pode variar dependendo do contexto. A execução contratual pode ser aplicada no caso de cadastro do paciente no banco de dados do prestador de serviço e na realização de cobrança pelo setor financeiro do estabelecimento. O legítimo interesse pode ser utilizado no envio de material de marketing, desde que respeite os critérios legais. O consentimento pode ser necessário em casos específicos, como a realização de cobrança por empresa terceirizada ou o pedido de aprovação da consulta ou procedimento para o plano de saúde. A adequada fundamentação legal e respeito aos direitos do titular são cruciais em cada situação.

b. Controlador/operador

Nas hipóteses de tratamento de dados cadastrais apontadas acima, os estabelecimentos de odontologia 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 é parceiro do laboratório) 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:

- 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;
- realização de cobrança pelo setor financeiro do estabelecimento – o prestador de serviços de saúde que determinou a cobrança do serviço poderá ser o controlador;

- 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;
- 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;
- 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 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 Odontológico e consulta

a. Introdução

A segunda etapa do atendimento do paciente envolve o tratamento de dados sensíveis, já que a prestação de serviços de saúde como atividade fim necessariamente envolve a coleta e manipulação de dados de saúde. Por esse motivo, essa fase pode ser considerada a mais sensível do tratamento de dados realizado no atendimento.

Nesse contexto, os principais pontos de atenção relacionados ao tratamento de dados pessoais realizados com o prontuário do paciente estão descritos nos diplomas normativos mencionados anteriormente. Esses pontos incluem:

a) Acesso e manuseio das informações do prontuário odontológico por profissionais de saúde: Profissionais envolvidos no tratamento do paciente são obrigados ao sigilo profissional, o que significa que devem manter a confidencialidade das informações contidas nos prontuários. O acesso a essas informações devem ser restrito apenas aos profissionais autorizados, e medidas de segurança devem ser adotadas para proteger a privacidade dos dados.

b) Hospedagem dos prontuários por terceiros: Caso os prontuários sejam armazenados em sistemas gerenciados por terceiros, é essencial garantir que esses fornecedores sigam as

normas de segurança e privacidade necessárias. Contratos e acordos específicos podem ser estabelecidos para garantir a conformidade com as regulamentações de proteção de dados.

c) Utilização do prontuário laboratorial para gerar diagnósticos com auxílio de softwares: O uso de softwares para análise de prontuários laboratoriais deve ser realizado de maneira ética e respeitando a privacidade do paciente. É fundamental garantir que esses sistemas estejam em conformidade com as normas de proteção de dados e que medidas apropriadas de segurança sejam implementadas.

d) Acessar informações do prontuário odontológico por profissional da saúde obrigado ao sigilo profissional em caso de risco de vida: Em situações emergenciais que envolvam risco de vida, é possível que informações do prontuário odontológico sejam acessadas por profissionais da saúde obrigados ao sigilo profissional. Contudo, essa ação deve ser justificada pela necessidade de proteger a vida do paciente, e medidas adicionais podem ser adotadas para garantir a segurança e a privacidade dos dados.

Esses pontos destacam a importância de as instituições de saúde adotarem práticas e políticas que assegurem a proteção dos dados sensíveis dos pacientes, respeitando normas éticas e regulamentações específicas do setor.

b. Controlador/operador

Nas hipóteses de tratamento dos dados do prontuário laboratorial apontadas acima, os profissionais de saúde responsáveis pelo atendimento e posterior preenchimento e manuseio do prontuário 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, um(a) assistente que manuseia o prontuário sob orientação da biomédica que efetivamente é a responsável pelo prontuário e

pelo paciente é apenas um(a) operador(a). Isso porque, ainda que ele(a) manuseie e preencha o documento, quem detém o poder decisório é a biomédica, ainda que tanto o/a biomédica quanto o/a assistente possua o dever de sigilo profissional.

Já no caso do estabelecimento (pessoa jurídica) no qual a biomédica 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/a biomédica 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: biomédica e estabelecimento no qual o/a biomédica atua podem ser considerados controladores e os/as assistentes 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(a) biomédica ou estabelecimento no qual o/a dentista 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 odontológicos, 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 odontológico por profissionais de saúde envolvidos no tratamento do paciente que são obrigados ao sigilo profissional”; “utilização do prontuário odontológico para gerar diagnósticos com auxílio de softwares”; “acessar informações do prontuário odontológico 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 odontológico por profissionais não obrigados ao sigilo profissional" deve ser realizado com o consentimento do usuário ou por obrigação legal ou regulatória.

d. Período de armazenamento/ eliminação

O período de armazenamento de dados deve seguir o princípio da minimização, garantindo que os dados sejam mantidos apenas enquanto forem pertinentes, adequados e limitados aos fins para os quais são processados. Embora a LGPD não estabeleça um período específico para o armazenamento dos dados, ela enfatiza a importância de eliminar os dados quando não forem mais necessários para a finalidade original.

No contexto de dados de saúde, a Lei nº 13.787/2018 estabelece diretrizes específicas para a digitalização e o armazenamento de prontuários de pacientes. De acordo com essa lei, os prontuários devem ser preservados por um período mínimo de 20 anos. Além disso, o processo de eliminação desses dados deve ser conduzido de maneira a resguardar a intimidade do paciente e garantir o sigilo das informações.

Portanto, ao lidar com dados de saúde, as instituições de saúde devem adotar práticas que estejam em conformidade não apenas com a LGPD, mas também com regulamentações específicas do setor, como a Lei nº 13.787/2018. Essas práticas devem incluir políticas claras sobre o período de retenção de dados, os métodos de eliminação e as medidas de segurança necessárias para proteger a privacidade e o sigilo das informações dos pacientes.

e. 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 desempenham um papel crucial na geração e gestão de dados sensíveis de saúde, apresentando desafios específicos relacionados ao tratamento dessas informações. Além dos riscos comuns aos estabelecimentos de saúde, como o manejo adequado de dados cadastrais e prontuários, os laboratórios enfrentam particularidades relacionadas aos exames laboratoriais. Destacar essas especificidades é essencial para garantir o cumprimento das normas de proteção de dados.

É importante notar que, além da equipe médica e técnicos de enfermagem, os laboratórios contam com a participação de farmacêuticos especializados em análises clínicas. Esses profissionais também são regidos por normas específicas, como a Resolução do Conselho Federal de Farmácia nº 596/2014, que estabelece diretrizes para o dever de sigilo.

O Protocolo de Compartilhamento aborda o cenário em que os resultados dos exames laboratoriais são compartilhados com outros prestadores de serviços de saúde. No entanto, a gestão desses dados vai além das preocupações comuns, pois os resultados dos exames contribuem para a formação de grandes bancos de dados de saúde. Isso demanda cuidados adicionais, especialmente considerando a sensibilidade e o potencial impacto dessas informações na saúde dos pacientes.

Os exames laboratoriais passam por diversas fases, desde a coleta das amostras até o armazenamento dos resultados. Cada etapa do processo envolve o tratamento de dados sensíveis, desde a identificação do paciente até a divulgação do resultado. A conformidade com a LGPD e outras regulamentações relacionadas à proteção de dados é crucial em todas essas fases.

Em resumo, os laboratórios de análises clínicas devem implementar medidas específicas para proteger a privacidade e a segurança dos dados sensíveis de saúde, desde a coleta até o armazenamento e compartilhamento. Essas medidas devem levar em consideração as diretrizes da LGPD, bem como normas setoriais e regulamentações específicas que regem o setor de saúde e análises clínicas.

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”; “encaminhamento da amostra 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.

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 é necessário que se observe o previsto na Lei no 13.787/2018 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.

e. Controlador/operador

O Laboratório São Geraldo 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.

f. Base legal

Além das bases legais já informadas, requer-se atenção especial à utilização dos dados coletados. 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 Nº 226/2020 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.

g. Sigilo/segurança da informação

Assim como no protocolo referente ao tratamento dos dados do prontuário laboratorial, as medidas de segurança relativas aos dados gerados pela Laboratório São Geraldo, devem ser reforçadas, tendo em vista que dados sensíveis do paciente são 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 Laboratório São Geraldo 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 odontológica, 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).

No Laboratório São Geraldo, 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 conexão com o paciente/outros dentistas, 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.

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 uma 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 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 laboratórios parceiros e convênios, com o objetivo de facilitar o intercâmbio das informações, em prol do paciente; ou o compartilhamento de prontuários e resultados de exames pelo dentista com um hospital/clínica, por exemplo, para realização de procedimentos cirúrgicos.

Tais situações diferem do compartilhamento realizado entre dentistas, 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.

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 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 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 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 estabelecimentos de saúde

a. Introdução

A hipótese de compartilhamento de dados entre estabelecimentos de saúde envolve a troca de informações entre duas pessoas jurídicas do setor de saúde. Isso pode ocorrer, por exemplo, quando hospitais, clínicas ou outros estabelecimentos precisam compartilhar informações sobre o estado de saúde de pacientes para facilitar o remanejamento ou a continuidade do atendimento.

Esse tipo de compartilhamento de dados é comum no setor de saúde, onde a colaboração entre diferentes entidades é essencial para garantir a prestação adequada de serviços e o cuidado contínuo aos pacientes. No entanto, é fundamental que esse compartilhamento esteja em conformidade com as leis de proteção de dados, como a LGPD (Lei Geral de Proteção de Dados), para garantir a privacidade e a segurança das informações dos pacientes.

As entidades envolvidas nesse compartilhamento devem seguir práticas seguras de manuseio de dados, garantindo que apenas as informações necessárias sejam compartilhadas e que o acesso seja restrito a profissionais autorizados. Além disso, é importante que o

compartilhamento de dados seja realizado com base em uma justificativa legal, como o cumprimento de obrigações legais ou regulatórias, a tutela da saúde, o exercício regular de direitos, entre outros fundamentos previstos na LGPD.

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 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 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.

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 do CFO nº 91/2009, cujo tempo mínimo para a manutenção de prontuários (odontológicos) em suporte de papel ou digitais são de 10 (dez) anos. Atenção: muito embora o CFO estipule o tempo mínimo de 10 anos, recomenda-se guardar o prontuário indefinidamente. Isso pois existem alguns riscos jurídicos em se descartar o prontuário, mesmo após os 10 anos. Eis alguns deles: a) O paciente pode alegar em processos judiciais vício oculto (defeito que só se manifesta após certo tempo, sendo de difícil constatação pelo consumidor), ainda que fora deste prazo acima. Nesse caso, o prazo prescricional só se inicia a partir do momento em que o vício pôde ser detectado pelo consumidor – o que pode levar mais de 10 anos. b) O prazo de prescrição para a reparação de danos não corre contra os absolutamente incapazes (conforme arts. 3º e 198 do Código Civil). c) Em relação a doenças

que o cirurgião-dentista poderia ter diagnosticado e sugerido tratamento a tempo, mas não o fez, também há um complicador. Isso porque o dentista pode ser condenado muitos anos depois de findo o tratamento, com base na teoria jurídica francesa, também adotada no Brasil, da “Perda de uma Chance”. Para defender-se, pode ser necessário apresentar documentos antigos. Por todos esses motivos é que não se recomenda o descarte dos prontuários odontológicos

Assim, os prontuários dos pacientes devem ser preservados por, no mínimo, 10 anos e o processo de eliminação deverá resguardar a intimidade do paciente e o sigilo das informações.

2.4. 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) informações e documentos utilizados na instrução e defesa em processos administrativos sancionadores por infrações à normas da saúde suplementar; (iv) 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

Com efeito o Laboratório São Geraldo deve seguir tais premissas em respeito a ANS, sendo que para tanto, 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 deste Laboratório.

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. 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 de estes 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.

c. Base legal

O Laboratório São Geraldo com base nas diretrizes da ANS e na própria LGPD (LEI 13.709/2018) 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).

d. 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 do CFO nº 91/2009, cujo tempo mínimo para a manutenção de prontuários em suporte de papel ou digitais são de 10 (dez) anos. Atenção: muito embora o CFO estipule o tempo mínimo de 10 anos, recomenda-se guardar o prontuário indefinidamente. Isso pois existem alguns riscos jurídicos em se descartar o prontuário, mesmo após os 10 anos. Eis alguns deles: a) O paciente pode alegar em processos judiciais vício oculto (defeito que só se manifesta após certo tempo, sendo de difícil constatação pelo consumidor), ainda que fora

deste prazo acima. Nesse caso, o prazo prescricional só se inicia a partir do momento em que o vício pôde ser detectado pelo consumidor – o que pode levar mais de 10 anos. b) O prazo de prescrição para a reparação de danos não corre contra os absolutamente incapazes (conforme arts. 3º e 198 do Código Civil). c) Em relação a doenças que o cirurgião-dentista poderia ter diagnosticado e sugerido tratamento a tempo, mas não o fez, também há um complicador. Isso porque o dentista pode ser condenado muitos anos depois de findo o tratamento, com base na teoria jurídica francesa, também adotada no Brasil, da "Perda de uma Chance". Para defender-se, pode ser necessário apresentar documentos antigos. Por todos esses motivos é que não se recomenda o descarte dos prontuários.

Assim, os prontuários dos pacientes devem ser preservados por, no mínimo, 10 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.

2.5. Compartilhamento entre estabelecimento de saúde e operadoras

Ainda que o compartilhamento entre estabelecimentos de saúde e operadoras de planos de saúde/odontológicos 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 destesdados;	- 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

- Retenção dos dados pelo período necessário; - Adotar medidas de segurança da informação	

2.6. 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 protocolos laboratoriais ou do estabelecimento de saúde para atender ordem judicial ou para defesa própria; c) Compartilhar informações do exames 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 biomédico 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 realizado 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 laboratoriais ou de saúde em geral - nesse caso é capital atentar para o contexto específico, sendo possível que a empresa responsável pelo desenvolvimento dos dispositivos seja controladora 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, consultando sempre o comitê de segurança da informação ou o seu jurídico ou o seu DPO aténs da tomada de decisão de compartilhamento dos dados.

c. Períodos de armazenamento / eliminação

O período de armazenamento de dados deve aderir ao princípio da minimização, que preconiza que os dados devem ser mantidos apenas enquanto forem pertinentes, adequados e limitados aos fins para os quais são processados. A eliminação dos dados deve ocorrer assim que estes não atendam mais aos princípios da finalidade e da necessidade, conforme estabelecido no art. 6º da LGPD.

Especificamente em relação aos dados de saúde, é crucial observar o disposto na Lei nº 13.787/2018 e na Resolução do CFO nº 91/2009. Conforme essas normativas, o tempo mínimo de manutenção de prontuários, seja em suporte de papel ou digitais, é de 10 (dez) anos. Importante ressaltar que, embora o CFO estipule esse tempo mínimo, é recomendável guardar os prontuários indefinidamente devido a riscos jurídicos, como a alegação de vício oculto por parte do paciente.

Alguns dos riscos jurídicos que justificam a prática de manter os prontuários por tempo indeterminado incluem a possibilidade de alegações de vício oculto em processos judiciais, o prazo de prescrição que não corre contra os absolutamente incapazes, e a teoria jurídica da "Perda de uma Chance" em casos relacionados a doenças que poderiam ter sido identificadas e tratadas a tempo.

Assim, o laboratório deve preservar os prontuários dos pacientes por, no mínimo, 10 anos, seguindo as disposições legais. O processo de eliminação deve ser conduzido com cuidado, resguardando a intimidade do paciente e o sigilo das informações, mesmo quando realizado por órgãos públicos. A recomendação de manter os prontuários indefinidamente se baseia na prevenção de riscos legais associados à prescrição de possíveis ações judiciais, protegendo tanto o laboratório quanto os interesses dos pacientes.

d. 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.

e. Privacy by design

Recomenda-se, para o desenvolvimento e implementação de novas tecnologias e metodologias nesta fase, que se observe a 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"15, com as seguintes orientações que os fabricantes de dispositivos médicos devem considerar em seus projetos:

(i) 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;

- 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

(ii) 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

(iii) 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.

(iv) 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.

(v) 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.

(vi) 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

(vii) Confiabilidade e disponibilidade

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

f. Período de armazenamento

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 do CFO nº 91/2009, cujo tempo mínimo para a manutenção de prontuários em suporte de papel ou digitais são de 10 (dez) anos. Atenção: muito embora o CFO estipule o tempo mínimo de 10 anos, recomenda-se guardar o prontuário indefinidamente. Isso pois existem alguns riscos jurídicos em se descartar o prontuário, mesmo após os 10 anos. Eis alguns deles: a) O paciente pode alegar em processos judiciais vício oculto (defeito que só se manifesta após certo tempo, sendo de difícil constatação pelo consumidor), ainda que fora deste prazo acima. Nesse caso, o prazo prescricional só se inicia a partir do momento em que o vício pôde ser detectado pelo consumidor – o que pode levar mais de 10 anos. b) O prazo de prescrição para a reparação de danos não corre contra os absolutamente incapazes (conforme arts. 3º e 198 do Código Civil). c) Em relação a doenças que o cirurgião-dentista poderia ter diagnosticado e sugerido tratamento a tempo, mas não o fez, também há um complicador. Isso porque o dentista pode ser condenado muitos anos depois de findo o tratamento, com base na teoria jurídica francesa, também adotada no Brasil, da “Perda de uma Chance”. Para defender-se, pode ser necessário apresentar documentos antigos. Por todos esses motivos é que não se recomenda o descarte dos prontuários.

Assim, os prontuários dos pacientes devem ser preservados por, no mínimo, 10 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.

3. 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 Odontológica do CFO (RESOLUÇÃO 118/2012) trata da matéria, prevendo práticas vedadas ao dentista 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. O CONEP16 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 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 de uma pandemia). 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 perspectivas17 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 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 a 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.

Por isso esse protocolo dedica-se 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.

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 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 de o 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"18 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 Esclarecido (TCLE), auxiliando no cumprimento dos princípios da transparência e do consentimento como manifestação livre, informada e inequívoca do titular.

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.

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.

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.

Acresce-se, ser 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.

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.

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.

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

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, conforme elucida o Código de Boas Práticas da Confederação Nacional de Saúde.

Destacamos 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).

4.1. Direito de 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, é tão forte, de modo que a recusa em prestar as informações solicitadas deve ocorrer 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 informações adicionais 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. Direito de 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. Direito de 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. Direito de 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

Conforme estabelecido nos artigos 9º e 18 da Lei Geral de Proteção de Dados (LGPD), você, como titular dos dados, possui os seguintes direitos:

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 a LGPD;
V. Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, observados segredos comercial e industrial;
VI. Eliminação dos dados pessoais tratados com seu consentimento, 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.

Este formulário tem como propósito auxiliar você no exercício desses direitos. Se necessário, solicitamos que seja encaminhada uma cópia deste formulário para outros prestadores de serviços de saúde nos quais você imagina 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 celular:
- Telefone fixo:
- E-mail:

SOLICITAÇÃO

( ) ACESSO

( ) RETIFICAÇÃO

( ) CANCELAMENTO ( ) OPOSIÇÃO

Descrição da Informação Solicitada:

Por favor, forneça detalhes sobre a informação específica que motiva esta solicitação. Quanto mais detalhes fornecidos, mais preciso será nosso processo de busca e resposta.

Documentos que Subsidiem o Pedido:

Caso haja documentos específicos que possam apoiar ou esclarecer sua solicitação, pedimos que os identifique aqui. Isso ajudará na análise e agilizará o processo de fornecimento da informação.

Declaração:

Declaro, sob as penalidades da lei, que as informações apresentadas neste formulário são verdadeiras e que sou a pessoa a quem elas se referem, conforme comprovado pelo documento de identidade com foto anexado a este pedido.

_____ de _____ de _____

_____

Assinatura do requerente

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.

Por meio deste são adotadas 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.

Política e Conscientização	Criar, revisar e comunicar diretrizes considerando melhores práticas para assegurar a proteção e privacidade dos dados pessoais
Gestão de identidades e acesso	Fornecer acessos somente as pessoas autorizadas e revogá-los quando a pessoa não trabalhar mais na empresa. Proteger os logins deacesso evitando a exposição desses acessos a pessoas não autorizadas. Adotar um segundo fator de autenticação sempre que possível
Gestão de Backups	Garantir que os dados relevantes para o negócio tenham uma cópia de segurança, devidamente protegida contra acessos nãoautorizados
Gestão de Ativos	Inventariar os ativos que tratam dados pessoais e garantir os requisitos mínimos de segurança
Gestão de SegurançaEndpoint	Garantir que todos os ativosque tratam dados pessoais tenham uma solução de antimalware instalada e atualizada periodicamente

Assim, foi concretizado, após a realização do mapeamento do fluxo de tratamento dos dados pessoais, foram identificados os principais componentes para que as implementações de segurança sejam realizadas de forma mais efetiva. Para tanto, foram adotados e utilizados os controles de segurança especificados no NIST Cybersecurity Framework e normativas ISO 27701 /27001.

REQUISITOS DE SEGURANÇA MÍNIMOS

REQUISITOS DE SEGURANÇA PRIORITÁRIOS

Monitoramento e Gestãode 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 sejamregistrados 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	Garantir a segurança do acesso físico às informaçõestratadas em mídias eletrônica, papel e sistemas
Gestão de Vulnerabilidade / Pentes	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.
Transferênciade Dados	Garantir a segurança na comunicação durante os processos de transferênciasde dados.
Exclusão de DadosTratados	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 está integrado 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.

Observa-se que os requisitos mencionados delineiam um cenário ideal, abrangendo diversos aspectos cruciais a serem observados pelos prestadores de serviços de saúde. No entanto, é imperativo levar em conta o atual estágio de adequação de cada estabelecimento e os tipos de sistemas empregados para o tratamento de dados de saúde ao elaborar a estratégia de segurança da informação.

Atenciosamente,

Laboratório São Geraldo
15 de maio de 2024.