GUIA LGPD

INDÚSTRIA FARMACÊUTICA

SINDUSFARMA

INTERFARMA
Associação da Indústria Farmacêutica de Pesquisa

GUIA LGPD

INDÚSTRIA FARMACÊUTICA

GUIA LGPD

INDÚSTRIA FARMACÊUTICA

SINDUSFARMA

Setembro
2020

INTERFARMA
Associação da Indústria Farmacêutica de Pesquisa

SUMÁRIO

APRESENTAÇÃO

O presente Guia LGPD destina-se às empresas do setor farmacêutico associadas ao SINDUSFARMA – Sindicato da Indústria de Produtos Farmacêuticos e à INTERFARMA – Associação da Indústria Farmacêutica de Pesquisa. O documento foi elaborado a partir do trabalho original de consultoria realizado pelo escritório Chenut Oliveira Santiago Sociedade de Advogados, sob a coordenação do Dr. Fernando Santiago, posteriormente modificada e adaptada por colaboradores de um grupo de associadas.

A Lei 13.709/18, e seguintes modificações, inaugurou um novo cenário no ordenamento jurídico brasileiro no que se refere a proteção das informações pessoais de todos brasileiros. Em que pese existirem leis e normativas que, em maior ou menor medida, já oferecessem proteção jurídica às informações pessoais, é inegável que a nova Lei estabeleceu novo modelo jurídico regulatório ao país.

Como não poderia deixar de ser o texto ora apresentado não tem caráter vinculante. Trata-se de uma construção voltada para nortear quem terá que se sujeitar à nova realidade, de um lado, e trazer a conhecimento da sociedade certas particularidades do setor neste tema, de outro. Seu objetivo é simplesmente orientar as Associadas quanto às regras existentes na LGPD, com ênfase em áreas corporativas inerentes ao setor econômico, dentre elas a de farmacovigilância, pesquisa clínica, relacionamento com pacientes e profissionais da saúde.

Diante dessa finalidade, o Guia traz aos Associados uma visão instrumental da LGPD, com recomendações específicas para a adequação da Indústria Farmacêutica em relação àquele referencial.

Assim, O SINDUSFARMA e a INTERFARMA esperam que o Guia contribua com a adequação das suas associadas e com o debate sobre a compreensão da aplicação da LGPD a o setor farmacêutico no Brasil.

DEFINIÇÕES

i. **Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável.

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

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

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

v. **Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

vi. **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

vii. **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

GUIA LGPD – Indústria Farmacêutica

viii. **Encarregado:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

ix. **Agentes de tratamento:** o controlador e o operador.

x. **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.

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

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

xiii. **Bloqueio:** suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

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

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

xvi. **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;

xvii. **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;

xviii. **Autoridade nacional:** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

xix. **Teste de Legítimo Interesse:** teste a ser realizado em determinadas circunstâncias, quando a base legal do tratamento seja "interesse legítimo do controlador ou de terceiros", tendo por objetivo avaliar os impactos aos direitos e liberdade do titular, bem como as expectativas razoáveis deste em relação ao tratamento de seus dados pessoais.

1
O QUE É A LEI GERAL DE PROTEÇÃO DE DADOS?

A Lei Geral de Proteção de Dados – LGPD, Lei Federal nº 13.709, de 14 de agosto de 2018, tem como finalidade disciplinar o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Na exposição de motivos do Projeto de Lei de que originou a LGPD – PL nº 4.012/2012- explicita-se a preocupação com a forma como os dados pessoais vinham sendo tratado no Brasil, sobretudo diante do avanço tecnológico dos últimos anos.

Foi a partir dessas premissas que o Congresso Nacional e o Presidente da República aprovaram a LGPD, que busca, antes que tudo, assegurar a dignidade da pessoa humana por meio da proteção à sua intimidade e privacidade.

2
OS PRINCÍPIOS DA LGPD

São princípios básicos dos Titulares de Dados Pessoais e que deverão ser observados por todos:

i. **Boa-fé:** a boa-fé é comumente interpretada como sendo a atitude que se espera de um indivíduo mediano, pautado nos valores sociais e conduta ética esperadas de uma sociedade.

ii. **Finalidade:** a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

iii. **Adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

iv. **Necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

v. **Livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

vi. **Qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

vii. **Transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

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

ix. **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

x. **Não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

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

3 AÇÕES ESTRUTURANTES PARA O ATENDIMENTO DA LGPD

3.1. Indicação de Encarregado pelo tratamento dos dados pessoais (*Data Protection Officer* – DPO)

A LGPD impõe ao Controlador a obrigação de nomear um Encarregado pelo tratamento dos dados pessoais – ETD, mais conhecido pelo termo em língua inglesa "Data Protection Officer (DPO)" (art. 41).

Inicialmente, o texto da LGPD associava a figura do Encarregado unicamente ao Controlador. Contudo, a redação atual da LGPD permite a nomeação deste importante profissional pelo "Operador" (art. 5º, VIII).

A indicação de um Encarregado tem o objetivo de atribuir a uma determinada pessoa física ou jurídica a responsabilidade pela iniciativa, centralização e coordenação de todas as ações necessárias à implementação de um projeto complexo de adequação à LGPD.

Os critérios de nomeação e de dispensa do Encarregado serão objeto de regulamentação pela futura Autoridade Nacional de Proteção de Dados (ANPD), considerando a natureza, o porte da entidade ou o volume de operações de tratamento de dados.

Nos termos da LGPD, o Encarregado possui as seguintes atribuições:

3.1.1. Aceitar reclamações e comunicações dos Titulares, prestar esclarecimentos e adotar providências;

3.1.2. Receber comunicações da Autoridade Nacional e adotar providências;

3.1.3. Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

3.1.4. Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

3.2. A elaboração de Registro de Tratamento dos Dados Pessoais

A elaboração e a manutenção de um registro de tratamentos são elementos estruturantes da maior importância, sendo obrigatória a sua conservação para fins de controle interno, auditoria e fiscalização (art. 37).

O registro de tratamentos proporciona às empresas a tomada de conhecimento sobre a forma como trata os dados pessoais em suas múltiplas atividades, gerando conhecimento e visão global sobre as atividades e departamentos da empresa.

Ao oferecer uma visão global sobre a empresa, o registro representa uma ferramenta extremamente útil, sendo o ponto de partida para qualquer ação ou investigação relacionada a dados pessoais, sobretudo para os casos de incidentes.

Dessa forma, cada atividade ou ação envolvendo dados pessoais dentro da empresa deve estar representada por um registro de tratamentos. Considerando a novidade do procedimento, sugere-se que a sua elaboração inicial seja confiada aos responsáveis pela execução das referidas atividades com o auxílio do Encarregado ou de profissionais especializados. Após a estruturação da primeira versão e mediante o aumento do conhecimento e da compreensão dos envolvidos sobre o documento, a sua atualização constante pode ser feita regularmente pelos executores da atividade retratada no registro, inexistindo modelo obrigatório para a sua realização.

Para o registro, têm-se como referência as informações mínimas:

3.2.1. Atividade objeto do registro;

3.2.2. Objetivos perseguidos – descrever a finalidade do tratamento;

3.2.3. Categorias de pessoas envolvidas – titulares dos dados pessoais;

3.2.4. Categorias de dados coletados – os tipos de dados envolvidos na atividade;

3.2.5. Períodos de retenção para cada categoria de dados;

3.2.6. Categorias de destinatários de dados;

3.2.7. Transferências de dados para o exterior;

3.2.8. Medidas de segurança;

3.2.9. Testes de Legítimo Interesse (TLI/LIA);

3.2.10. Relatório de impacto a privacidade de dados (RIPD/DPIA).

GUIA LGPD – Indústria Farmacêutica

3.3. Elaboração de Políticas Relacionadas ao Tratamento de Dados Pessoais

Importante elemento para a estruturação interna da empresa no cumprimento das normas previstas na LGPD é a criação de políticas e procedimentos que deverão ser observados por todos na empresa e por aqueles que com ela se relacione e que tenha interação com dados pessoais.

Entre políticas e procedimentos destacam-se **(i)** Política de Privacidade, **(ii)** Política de Proteção de Dados Pessoais, **(iii)** Política de Prazo de Retenção de Dados Pessoais, **(iv)** Política de Controle de Acesso e Circulação de Dados Pessoais e **(v)** Política de Compartilhamento de Dados Pessoais. Tais Políticas poderão dispor sobre os seguintes tópicos.

3.3.1. Política de Privacidade

i. Introdução;

ii. Finalidades específicas dos tratamentos;

iii. Forma e duração do tratamento;

iv. Identificação do controlador;

v. Informações de contato do controlador;

vi. Informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

vii. Responsabilidades dos agentes que realizarão o tratamento;

viii. Direitos do Titular.

3.3.2. Política de Proteção de Dados Pessoais

i. Os princípios básicos a serem observados para o tratamento de dados pessoais pela empresa;

ii. A forma de tratamento de dados sensíveis;

iii. O processamento de dados pessoais por operadores, (eventualmente com link para as cláusulas a serem inseridas nos contratos com terceiros);

iv. Como são tratadas as transferências de dados pessoais para países terceiros;

v. Os direitos dos Titulares dos dados pessoais;

vi. Os procedimentos para tratamento das reclamações dos Titulares de dados;

vii. A observação de regras relativas à privacidade desde a fase de concepção dos produtos e processos da empresa (*privacy by design*);

viii. As ocasiões nas quais deve-se realizar uma análise de impacto sobre a proteção de dados pessoais e outros.

3.3.3. Política de Prazo de Retenção de Dados Pessoais

O tempo de armazenamento poderá ser o legal ou o convencional, a depender da natureza dos dados. O prazo legal deverá seguir o tempo de guarda disposto em leis e regulamentos, quando for o caso, e o prazo convencional deve ser estipulado por cada empresa em função da natureza do tratamento.

A título de exemplo, um documento não relacionado ao FGTS ou INSS versando sobre o contrato de trabalho de um empregado

(ex.: atestado médico, autorização para descontos não previstos em lei, etc.) poderá ser arquivado por até 05 (cinco) anos durante a relação de emprego, e até 02 (dois) anos após a rescisão do contrato de trabalho. Tal prazo é determinado por lei (Constituição Federal, Art. 7°, XXIX e CLT, art. 11).

Por outro lado, há uma diversidade de tratamentos de dados pessoais cujo prazo de arquivamento não é determinado por lei, como, por exemplo, o tempo de guarda dos dados pessoais de um prospecto comercial. Para tais dados – e na ausência de indicação pela autoridade reguladora – a empresa deverá estipular um prazo de guarda que seja coerente com as práticas de mercado e com a natureza do tratamento, justificando a razão do prazo adotado.

3.3.4. Política de Controle de Acesso Interno

Uma política de controle de acesso deverá ser realizada por cada empresa, respeitando o porte, o setor de atividade e estrutura, limitando o acesso ao banco de dados da empresa. Trata-se, pois, de determinar quais áreas – ou até mesmo quais postos de trabalho dentro de cada área – necessitam realmente ter acesso integral ou parcial ao banco de dados pessoais da empresa, e estruturar a implementação dessa compartimentação de acesso com o setor responsável pela tecnologia da informação.

Nesse sentido, a Política de Controle de Acesso Interno da empresa determina o perfil de acesso de cada área ao banco de dados da empresa – eventualmente com perfis de acesso distintos dentro de cada área, se for o caso, o procedimento a ser adotado em caso de necessidade de acesso a um dado pessoal bloqueado e a pessoa responsável pela análise desse pedido.

Com exemplo – exceto se as circunstâncias do caso concreto as justifiquem – o departamento pessoal de uma empresa não precisaria, em princípio, ter acesso à base de dados utilizada para prospecção comercial.

3.4. Adequação de Contratos

Acredita-se que toda empresa, em algum momento, compartilha dados pessoais. Dessa forma, é necessário que os contratos pelos quais o Controlador se relaciona com terceira pessoa estabeleça a qualificação das partes (controlador e operador) diante da LGPD, a confidencialidade específica sobre dados pessoais e a repartição de responsabilidades.

Vale lembrar que a LGPD responsabiliza todos os agentes de tratamento (controladores e operadores) pela segurança e garantia da integridade dos dados pessoais que tratam (art. 46), sendo que o Operador pode ser considerado solidariamente responsável com o Controlador caso descumpra a LGPD ou deixe de seguir as instruções lícitas instituídas por esse último (art. 47). A relação entre os agentes de tratamento, portanto, deve ser delimitada em instrumento contratual adequado.

3.5. Enquadramento do Fluxo Internacional de Dados Pessoais

Na possibilidade de a empresa transferir dados pessoais para o exterior, ela deverá seguir os requisitos previstos no art. 33 da LGPD.

Vale lembrar que a transferência internacional de dados é uma prática mais comum do que se imagina. Com efeito, as empresas frequentemente contratam o armazenamento do seu banco de dados ou de e-mails em servidores (*clouds*) situados no exterior.

O tema ainda necessita de regulamentação pela Autoridade Nacional de Proteção de Dados, a ser criada pelo Governo Federal. Contudo, a título exemplificativo, a transferência internacional de dados poderá ocorrer:

i. com o consentimento para tal ato, outorgado pelo titular dos dados pessoais transferidos, (em destaque e com informação prévia do caráter internacional da operação).

ii. mediante a redação de cláusula contratual específica com o destinatário dos dados no exterior contemplando as garantias do cumprimento dos princípios, dos direitos do titular, e do regime de proteção de dados previstos na LGPD (tal cláusula deverá ser adequada aos posicionamentos a serem emitidos posteriormente pela ANPD);

iii. em cumprimento de obrigação legal ou regulatória pelo controlador.

3.6. Mecanismos para Assegurar o Execício de Direito pelos Titulares dos Dados Pessoais

A LGPD trouxe uma série de novos direitos e garantias (sobretudo arts. 17 e 18) aos Titulares dos dados pessoais. A título de exemplo, os titulares dos dados pessoais podem solicitar a confirmação da existência de tratamento, a correção dos dados inexatos ou a sua eliminação, assim como a informação sobre as entidades públicas ou privadas com as quais o Controlador possa ter compartilhado os dados pessoais daqueles.

3.7. Treinamento para Conscientização dos Colaboradores

O princípio da necessidade é um dos princípios basilares da LGPD. Ele diz respeito essencialmente à qualidade dos dados pessoais tratados pelo Controlador. Este, por intermédio de seus colaboradores, deve ater-se à coleta e tratamento dos dados estritamente necessários à finalidade para a qual foram coletados.

A observância desse princípio implica na redução drástica da quantidade e do tipo de dados (qualidade) coletados, devendo-se eliminar todos os que não sejam essenciais para o atingimento da finalidade pretendida.

Nesse sentido, a organização de treinamentos para os colaboradores é um elemento essencial para o atingimento dos objetivos preconizados pela LGPD. A periodicidade desse treinamento dependerá do tamanho, do perfil, do volume de dados pessoais tratados e da periodicidade de renovação dos colaboradores de cada empresa. O respeito à norma é atingido mais facilmente quando ela é compreendida pelos responsáveis por sua aplicação.

GUIA LGPD – Indústria Farmacêutica

4
IMPLICAÇÕES DA LGPD SOBRE AS PRINCIPAIS ÁREAS DO SETOR INDUSTRIAL FARMACÊUTICO

4.1. Setor de Recursos Humanos

Em decorrência da quantidade e da diversidade dos dados pessoais que o setor de Recursos Humanos (RH) trata, ele se caracteriza como um dos mais afetados pela LGPD.

O setor de RH da empresa trata não só os dados pessoais dos colaboradores da empresa, mas também os de seus dependentes e os de candidatos a emprego. Tais dados frequentemente possuem natureza sensível (atestados médicos) ou dizem respeito a menores de idade (dependentes), o que reforça a necessidade do seu enquadramento e proteção.

Dessa forma, seguem abaixo os principais pontos que são submetidos ao RH, mas que podem variar em razão do seguimento, do porte, da origem e outros fatores inerentes à empresa.

4.1.1. Ampla Informação aos Titulares dos Dados Pessoais

Os empregados e terceirizados geridos pelo setor de RH devem receber uma nota de informação sobre o tratamento dos seus dados pessoais. Um meio simples e eficaz de atingir esse objetivo consiste, por exemplo, na fixação desse documento em locais estratégicos do local de trabalho ou ainda na divulgaçãoi por meio de redes internas da empresa. Gradualmente, tal notícia de informação deve ser incorporada aos novos contratos de trabalho ou de terceirização por meio da inclusão de cláusula específica sobre o tema.

Em relação ao aprendiz, as informações sobre o tratamento devem ser fornecidas de maneira simples, clara e acessível, consideradas suas características físicas, perceptivas, sensoriais, intelectuais e mentais, com uso de recursos audiovisuais quando adequado.

No mesmo sentido, os meios de coleta de dados pessoais dos candidatos a emprego devem contemplar informações sobre o tratamento dos dados pessoais, identificando a finalidade, o consentimento para eventual compartilhamento, se for o caso, assim como o prazo de retenção e os direitos conferidos ao Titular pela LGPD.

Caso haja câmeras de vigilância e geolocalização de determinada categoria de empregados é importante que tais tratamentos constem da notícia de informação que lhes seja destinada. Possivelmente este tema será objeto de regulamentação pela ANPD.

4.1.2. Segurança de Arquivos Físicos

Arquivos físicos do RH merecem atenção especial. Eles devem ser mantidos sob vigilância e com acesso restrito (inclusive, sendo o caso, dentro da equipe), até a sua adequada eliminação. Caso o local de estocagem destes arquivos sejam terceirizados, sugere-se que os contratos de terceirização prevejam mecanismos específicos de segurança e controle de acesso.

4.1.3. Dados Pessoais Sensíveis

Os dados pessoais sensíveis dos empregados ou dependentes coletados e tratados pelo Controlador também devem ser tratados com cuidado. Na maior parte das vezes, tais dados são obtidos no momento da contratação e ficam sob a guarda do setor de RH.

4.1.4. Dados de menores de idade

A coleta de dados pessoais de dependentes dos colaboradores é comum para fins de atribuições de diversos benefícios (planos de saúde, salário-família e outros). A LGPD impõe que o trfatamento seja realizado no melhor interesse da criança e do adolescente. Condições restritas para o tratamento dos dados de crianças, assim consideradas aquelas menores de 12 anos incompletos nos termos da legislação vigente. Nesses casos, uma boa prática consiste na obtenção do consentimento específico e em destaque por pelo menos um dos pais ou responsável legal para esse tratamento, ressaltando-se que tal consentimento pode ser obtido por meio de uma cláusula em destaque que integre o contrato de trabalho do responsável legal da criança.

Importante ressaltar; poderá haver situações que justifiquem o tratamento de dados de crianças, independentemente da obtenção do consentimento parental (por exemplo, para cumprimento de obrigação legal ou regulatória).

Em relação ao tratamento dos dados pessoais do "aprendiz", que pode eventualmente ser qualificado juridicamente como adolecente pela legislação, poderá ser fundamentado na execução do contrato de aprendizagem, sempre observando-se os detalhes do caso concreto.

5
SETOR ADMINISTRATIVO-FINANCEIRO

Como regra, o setor Administrativo-Financeiro é responsável por atividades relacionadas à controladoria, tesouraria e gestão de contas a pagar e a receber. Ainda que as atribuições desse setor variem consideravelmente entre as empresas, na maior parte dos casos os dados pessoais por ele tratados referem-se a empregados, representantes de seus clientes ou fornecedores.

Frequentemente, o departamento Administrativo-Financeiro compartilha dados pessoais com outras empresas, notadamente instituições financeiras e/ou empresas de análise de crédito e cobrança.

A diversidade das finalidades para as quais os dados pessoais são tratados pelo setor Administrativo-Financeiro ensejará, segundo o caso, hipóteses distintas de fundamentação legal. A título ilustrativo, há execução de contrato (remuneração), cumprimento de obrigação legal (Previdência Social), entre outras possibilidades.

GUIA LGPD – Indústria Farmacêutica

6
SETOR DE FARMACOVIGILÂNCIA E SAC

Os setores de Farmacovigilância, Qualidade e SAC frequentemente cumulam duas atividades semelhantes pela forma, mas distintas quanto ao seu conteúdo e sobretudo quanto à finalidade almejada. Tratam-se das atividades de Farmacovigilância ou Cosmetovigilância (segundo a atividade da empresa), e o Serviço de Apoio ao Cliente – SAC.

O setor de Farmacovigilância coleta dados pessoais sensíveis e, com grande frequência, realiza transferência internacional de dados. O Serviço de Atendimento ao Consumidor – SAC, destina-se essencialmente ao esclarecimento de dúvidas e reclamações de clientes, mas também serve como plataforma para relatos de efeitos adversos, atividade típica de farmacovigilância.

Desta forma, constata-se que a correta identificação do objeto do contato com a empresa, no menor lapso temporal possível, é de suma importância para o setor de Qualidade. A identificação precoce da natureza da chamada permite estruturar corretamente a forma e sobretudo o embasamento legal do tratamento dos dados pessoais efetuado.

6.1. Consentimento

Respeitando os princípios importos pela lei, o tratamento de dados pessoais – inclusive sensíveis – resultantes das atividades de Farmacovigilância e Cosmetovigilância não requer o consentimento do Titular dos dados, uma vez que se funda no cumprimento de uma obrigação legal ou regulatória.

O tratamento dos dados pessoais dos consumidores relacionados ao SAC, à exclusão dos relatos de efeitos adversos contendo dados referentes à saúde, poderá ser justificado pelo legítimo interesse. Sendo o direito da proteção dos dados pessoais de natureza extremamente casuística, não se pode excluir a necessidade eventual do consentimento, segundo o caso concreto e a qualidade do paciente (crianças e outros).

6.2. Prazo de Conservação de Dados Pessoais

Os dados pessoais tratados pelo sistema de farmacovigilância devem ser armazenados pelo período estabelecido na legislação aplicável ao tema, sobretudo os regulamentos editados pela Agência Nacional de Vigilância Sanitária.

Em relação aos dados pessoais coletados por meio do SAC sem relação com a atividade de farmacovigilância, as empresas devem determinar o seu prazo de armazenamento segundo as características do caso concreto.

6.3. Gestão dos Subcontratados

No caso de contratação de uma empresa para a realização das atividades de Farmacovigilância, Cosmetovigilância e de SAC e de Qualidade, conforme aplicável, o contrato deverá prever, além de cláusula específica sobre a confidencialidade dos dados pessoais, as demais cláusulas aplicáveis especificamente à proteção de dados pessoais, como a qualificação das partes (controlador ou operador), a repartição de responsabilidades, a gestão dos direitos dos titulares e outros.

6.4. Fluxo Internacional de Dados Pessoais

No caso de empresas multinacionais, é possível que relatos de eventos adversos e reclamações sobre a qualidade do produto sejam enviados para conhecimento e tratamento da matriz no exterior. Caso os dados pessoais enviados estejam anonimizados, não há qualquer exigência legal suplementar relacionada a essa transferência.

Contudo, caso seja possível a identificação do Titular, faz-se necessário a observância das regras previstas no art. 33 da LGPD assim como a regulamentação e orientações da ANPD sobre o tema.

Também poderá ser caracterizado transferência internacional de dados a contratação de terceira pessoa que armazene todo ou parte do banco de dados do Controlador em servidor localizado fora do Brasil, situação já destacada no subitem 3.5.

GUIA LGPD – Indústria Farmacêutica

7
SETOR COMERCIAL E MARKETING

O Setor Comercial e Marketing, por meio da Força de Vendas, frequentemente tem acesso a diversas categorias de dados pessoais, sobretudo àqueles de profissionais da área da saúde e médicos. Tais dados são utilizados tanto para fins de visitação dos referidos profissionais como para o envio de convites ou colaborações quando da realização de eventos, exposições, aulas, congressos e outros.

Vale salientar que, em determinadas empresas, as atividades e ações relacionadas à classe médica é subordinada a uma diretoria médica e não a comercial.

7.1. Dados de médicos e de clientes

Para fins da análise levada a efeito neste Guia, classificamos os profissionais relacionados à saúde em três categorias: **i)** os profissionais ou clientes que já têm contato regular com a empresa, **ii)** aqueles que estão sob contrato com a empresa, e **iii)** os prospectos.

i. *Profissionais relacionados à saúde ou clientes em contato regular com a empresa.*
Havendo atos voluntários que demostrem interesse nos produtos ou informações fornecidas pela empresa, é possível sustentar

o legítimo interesse como base legal para o tratamento dos dados pessoais não sensíveis, tanto destes profissionais quanto dos clientes (apoio e promoção de atividades do controlador).

ii. *Profissionais relacionados à saúde ou clientes sob contrato com a empresa*
O tratamento dos dados pessoais não sensíveis dos profissionais relacionados à saúde e de clientes pode, dentre outras possibilidades, ser fundado na execução do contrato (contrato de patrocínio, de fornecimento, etc). Contudo, se o tratamento envolver dados pessoais sensíveis deve-se analisar o caso concreto afim de identificar a base legal adequada.

iii. *Profissionais relacionados à saúde e clientes prospectos*
O tratamento de dados pessoais para fins de divulgação comercial devem ser analisados diante da situação concreta, sendo possível basear o tratamento dos dados pessoais no legítimo interesse da empresa, caso não haja o tratamento de dado pessoal sensível e esta base se mostre adequada após a realização do Teste de Legítimo Interesse. Dessa forma, ações específicas podem ser analisadas individualmente, levando-se em conta o tipo de dados tratados e a sua fonte primária, notadamente se adquiridos de empresas especializadas. Sobre o tema, vale ressaltar que informações anonimizadas ou estatísticas sobre produtos prescritos em determinada zona geográfica não são dados pessoais para fins da LGPD.

7.2. Privacy by Design

O departamento Comercial, Médico, Acesso e de Marketing estão, frequentemente, à frente de reflexões sobre novos projetos e estratégias de comunicação. Nesse sentido, cumpre ressaltar a importância da incorporação do princípio de *privacy by design* na idealização de tais projetos. Trata-se de levar em consideração as normas sobre privacidade preconizadas pela LGPD desde a concepção das novas ações, projetos e produtos idealizados pela empresa. A observação deste princípio na origem evita a modificação posterior dos processos visando adequá-los à lei.

8
SETOR MÉDICO E DE PESQUISA CLÍNICA

As atividades dos setores Médico e de Pesquisa Clínica levadas em conta para fins desse Guia consistem na: **i)** contratação de estudos clínicos, **ii)** gestão da relação com a classe médica, e **iii)** gestão de programas de suporte a pacientes.

A pesquisa clínica é um assunto bem regulamentado no Brasil. Os dados pessoais tanto dos médicos envolvidos nos estudos quanto aos dos pacientes são enquadrados pelos Comitês de Ética em Pesquisa (CEPS), pelo Conselho Nacional de Saúde (CNS), pelo Comissão Nacional de Ética em Pesquisa (CONEP) e pela Anvisa.

Frequentemente, parte substancial das pesquisas clínicas é terceirizada a uma Organização Representativa de Pesquisa Clínica – ORPC (ou Contract Research Organization – CRO, em inglês). Nesses casos, o Patrocinador não tem acesso à identificação dos pacientes envolvidos na pesquisa, posto que os dados são pseudonimizados. Os pacientes são mencionados na Ficha Clínica eletrônica de estudo por meio de um código suscetível de identificação unicamente pela sua confrontação com o Termo de Consentimento Livre e Esclarecido, cuja guarda é de responsabilidade da Instituição de Pesquisa. Assim, tal

cenário não nos parece implicar maiores desafios para os Associados em relação à gestão dos dados pessoais envolvidos nessa atividade.

Por outro lado, tanto as ORPC como as empresas que internalizam integralmente os estudos clínico devem adotar métodos adequados para garantir a segurança dos seus bancos de dados, assim como a anonimização dos dados pessoais tratados, sempre que possível.

Em relação aos Programas de Suporte ao Paciente – PSP, constata-se que essa denominação genérica engloba algumas práticas bem distintas. Para determinadas empresas, o PSP consiste na doação de medicamentos para que profissionais de saúde contratados por outras instituições (associações, empresas terceirizadas e outros.) empreguem em pacientes por eles selecionados. Nesse modelo, a empresa não tem acesso aos dados pessoais dos pacientes atendidos pela entidade responsável pelo Programa, recebendo unicamente um relatório com os dados pessoais dos médicos responsáveis pela aplicação, a quantidade de medicamentos fornecida e de pacientes atendidos.

Dentre outros casos, o PSP consiste na coleta de dados pessoais dos pacientes visando cadastrá-los em uma base de dados, oferecer-lhes descontos na aquisição de medicamentos e informações sobre saúde. Essa modalidade de programa requer mais atenção, uma vez que a empresa pode chegar a coletar e tratar dados pessoais referentes à saúde de uma quantidade significativa de pessoas.

Um dos primeiros pontos de atenção em relação aos programas atualmente em curso dizem respeito à informação dos Titulares de dados pessoais sobre os tratamentos realizados. Na maior parte dos casos a informação atualmente disponibilizada aos pacientes restringe-se às finalidades do tratamento, razão pela qual tais informações devem ser complementadas visando a sua adequação às exigências da LGPD (forma e duração do tratamento, informações acerca do uso compartilhado de dados, direitos dos Titulares, e outros).

9
SETOR DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO

As atividades dos setores relacionados a Tecnologia da Informação e Comunicação (TIC) levadas em conta para fins deste manual consistem na: **i)** Coleta e uso de dados pessoais para a gestão de acessos a Rede de dados, Aplicativos e Sistemas, **ii)** Mapeamento de ativos de informação e dados, **iii)** Segurança da Informação, **iv)** Plano de respostas a incidentes de Segurança de dados pessoais.

O setor de Tecnologia da Informação processa dados pessoais com a finalidade de cadastrar o acesso inicial a rede de dados da Companhia e permitir ao usuário mediante o uso de um ID (Identificador) e uma senha (Password) o acesso a diversos serviços como E-mail Corporativo, Internet, Intranet, Telefonia, Serviços de rede em geral e outros Sistemas/Aplicativos disponibilizados de acordo a necessidade e função desempenhada pelo colaborador/prestador de serviços.

Também compete ao setor de Tecnologia da Informação a manutenção e monitoramento dos diversos ativos da organização. É uma area

que acaba por relacionar-se com toda a organização e que muitas vezes conhece o processo das áreas em detalhes.

9.1. Coleta, uso e armazenamento de dados para acesso a rede e sistemas de informação

O tratamento de dados pessoais – inclusive sensíveis no caso de biometria resultantes das atividades de Tecnologia da Informação podem ser valer de algumas bases legais como: I – Consentimento II – Legítimo interesse do controlador e III – Execução de contratos. Importante ressaltar que se considera a possibilidade destas bases legais devido a necessidade de concessão de acesso a colaboradores (neste caso pode-se valer da base legal do legítimo interesse do controlador ou Execução de Contrato, salvo se não coletar dados biométricos que neste caso poderão exigir adicionalmente o consentimento do titular de dados – prestadores de serviços (Base legal do consentimento) visitantes que porventura necessitem de acesso a Rede WI-FI de visita (Base legal do consentimento).

Pontos que devem ser ressaltados neste tipo de tratamento de dados:

i. Coletar somente o mínimo necessário de dados pessoais para realização da finalidade.

ii. Considerar o local onde os dados serão armazenados (se existe transferência internacional de dados), devendo ser informado aos titulares de dados.

iii. Se os dados pessoais serão compartilhados com terceiros (para os casos em que a gestão dos acessos é realizada fora da organização ou que o sistema de gestão de acessos utiliza o modelo SaaS – Software as a Service). Necessário estabelecer cláusulas específicas de tratamento de dados.

iv. Período de retenção dos dados – estabelecer tabela de temporalidade com base em requisitos legais e regulatórios para esse tipo de dado pessoal.

v. Manter transparência na utilização dos dados para estas finalidades por meio de treinamentos, avisos, boletins informativos e outros.

9.2. Mapeamento de ativos de informação e dados

A área de Tecnologia da Informação é um importante ator no cenário da privacidade e proteção de dados, pois consegue auxiliar no entendimento das informações relevantes sobre componentes dos sistemas de informações através de seu CMDB (Configuration Management Database).

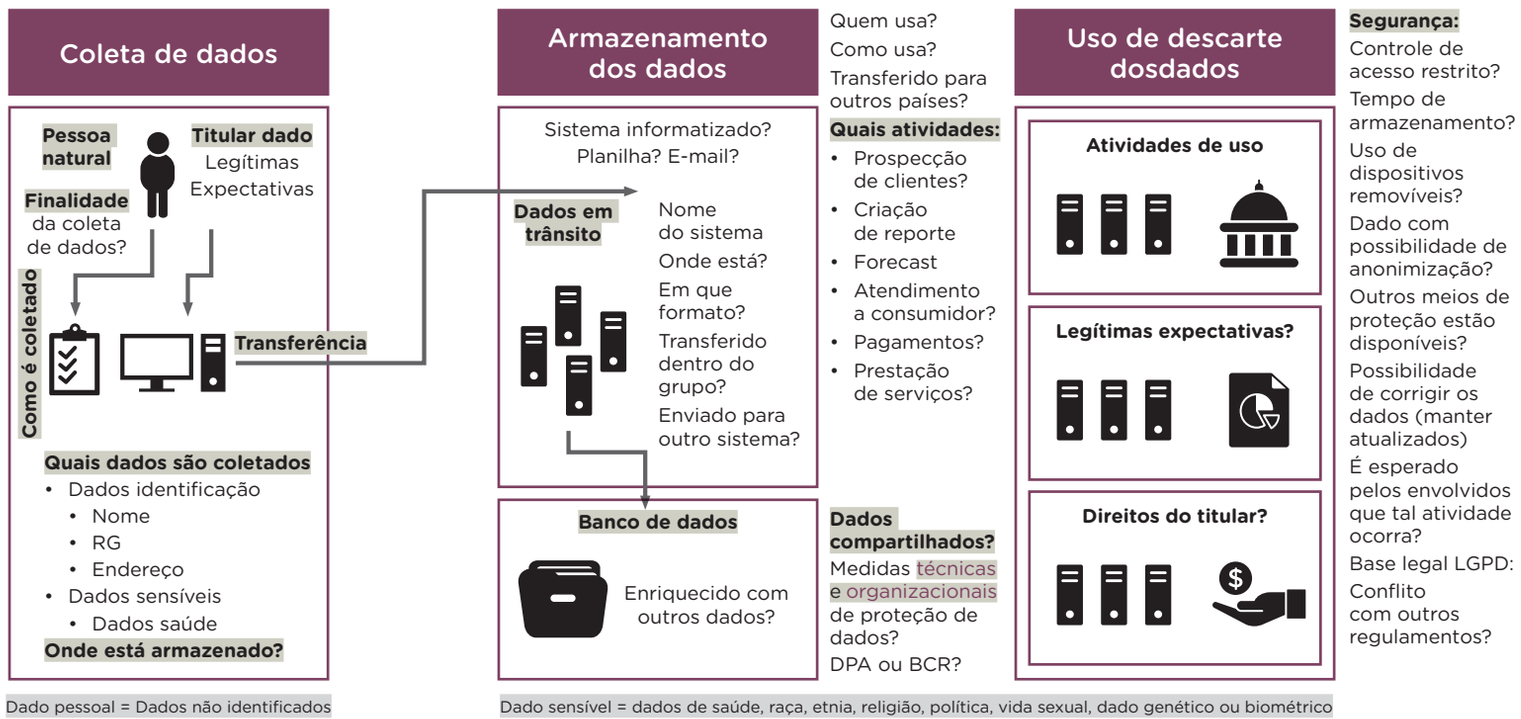
O CMDB oferece uma visão organizada dos dados e a interligação entre os diversos tipos de ativos como por exemplo (como, por exemplo, Sistemas, Hardware, Banco de dados, Localização, Classificação, Documentação dentro outros valiosos itens).

A combinação destas informação ao registro de tratamento de dados pessoais fornecerá uma visão final, a fim dos dados tratados pela organização possibilitando que os ajustes necessários sejam realizados para cumprir com os requerimentos legais e regulatórios das normas e leis de privacidade e proteção de dados.

Como exemplo, temos abaixo modelo de mapeamento para fins elucidativos:

CICLO DE VIDA DOS DADOS

Coleta, armazenamento, uso e descarte



GUIA LGPD – Indústria Farmacêutica

9.3. Segurança da informação

Importante conceituar inicialmente que a segurança da informação tem como base alguns pilares, assim como disciplinas que tratam temas específicos.

Os pilares da segurança da informação são:

i. **Confidencialidade** – Garantir que somente as pessoas autorizadas tenham acesso à informação.

ii. **Integridade** – Assegurar que os dados mantenham suas características originais ou que não sejam alterados sem a devida permissão e controle.

iii. **Disponibilidade** – Garantir que as informações estejam diponíveis para uso a qualquer momento.

Algumas das disciplinas de segurança da informação são:

i. **Gestão de acessos** – Disciplina que visa garantir que os acessos sejam controlados e monitorados. Alguns do temas que se destacam são: Autenticação, Autorização e Auditoria. Também vale ressaltar que a área de tecnologia possui em sua característica o acesso privilegiado de alguns de seus integrantes o que requer um controle adicional (conhecido como Gestão de Acessos Privilegiados) para garantir que somente pessoas devidamente autorizadas possam efetuar acessos com tal nível de permissão.

ii. **Gestão de vulnerabilidade em sistemas da informação** – O objetivo desta disciplina é agir de forma proativa mitigando possíveis falhas em sistemas ou arquiteturas de sistemas que possam comprometer a informação. O processo consiste em identificar, classificar e tratar as vulnerabilidades encontradas. Importante ressaltar que esta "priorização" tem como base a gestão de riscos que consiste em avaliar a "probabilidade" e o "dano" que uma vulnerabilidade pode causar no ativo e com base na nota de risco tomar decisão para minimizar, evitar, mitigar ou aceitar o risco identificado.

iii. **Criptografia** – Técnica que codifica os dados garantindo uma forte proteção durante o armazenamento e/ou trânsito dos dados. É uma tecnologia que requer a análise profunda antes do uso, pois existem pré-requisitos para a adoção de tais soluções que devem ser considerados: 1) Tipo de Criptografia (Chave Simétrica – uma mesma chave é utilizada para codificar e descodificar os dados – Chave Assimétrica, a chave utilizada para codificar os dados é diferente da que é usada para descriptografar os dados). Outro item importante é a gestão de tais chaves contra acesso não autorizado, perda ou roubo e que o processo deve estar em conformidade com o ICP – Brasil, que é o sistema nacional de certificação digital.

iv. **Anonimização** – Item comumente referenciado na LGPD para descaracterizar um dado como pessoal. Trata-se de recurso técnico que se caracteriza pela irreversibilidade do processo, de maneira que não haja condição razoável de retornar o estado original ou seja "dado pessoal". Algumas técnicas utilizadas para anonimização são: 1) Supressão de atributos – visa à remoção de uma secção ou coluna em base de dados no conjunto de dados. 2) Supressão do registro – Remoção de um registro inteiro do conjunto de dados. 3) Encobrimento de Caracteres – é a alteração de caracteres num valor dos dados por exemplo substituição por "*" ou "x". 4) Pseudonimizaçao – O dado perde a possibilidade de associação direta ou indireta a um indivíduo e somente pelo uso de informação adicional poderá ser identificado o titular do dado.

v. **Tópicos adicionais que requerem atenção:** 1) Políticas de segurança da informação que estabeleça regras e padrões para proteção

das informações. 2) Softwares de proteção contra Malwares. 3) Softwares para prevenção de vazamento de dados, conhecidos como DLP (Data loss prevention). 4) Seguros Cibernéticos (quando aplicáveis ao modelo e risco a que a empresa esta exposta) 5) Auditorias de segurança que possam identificar possíveis pontos de melhoria. 6) Análises de segurança da informação para sistemas críticos (Pentest – Testes que simulam ataques a sistemas e que permitem antecipar possíveis vulnerabilidades dos sistemas. Bug Bounty – Programa de premiação para pesquisadores e desenvolvedores que descobrem vulnerabilidades em aplicações e sistemas).

9.4. Plano de respostas a incidentes de segurança de dados pessoais

O plano de respostas a incidentes de segurança de dados pessoais é importante item no cumprimento dos requisitos da LGPD e consiste nas providências que serão adotadas pela organização ao ser identificado um incidente de segurança da informação que envolva dados pessoais.

Um incidente de segurança pode ser definido como um evento ou cadeia de eventos que comprometa a informação em um ou mais dos três pilares da segurança da informação (Confidencialidade, Integridade e Disponibilidade).

Destaca-se que para a LGPD somente serão considerados os casos que envolvam dados pessoais. Os tópicos abaixo trazem sugestões de possíveis passos básicos na adoção de um plano de respostas a incidentes de segurança de dados:

i. **Registro de operações de tratamento de dados pessoais** – A ideia é identificar a volumetria de dados, assim como a criticidade de tais dados e com isso priorizar as bases de dados que contenham "informações mais críticas";

ii. **Criação ou designação de um comitê de crises** – Identificar na organização setores e os respectivos gestores que devem fazer parte de um Comitê de atuação frente a uma crise de incidente de segurança da informação envolvendo dados pessoais. São exemplo os setores de RH, TI, Jurídico, Comunicação, Relação com Investidores, Segurança da Informação. Importante definir papéis e responsabilidades para cada membro deste Comitê de Crises.

iii. **Identificação prévia de fornecedores** – Definir a necessidade de utilizar serviços especializados com empresas terceirizadas, como: 1) Perícia Forense Computacional. 2) Serviços Jurídicos especializados. 3) Equipes de tecnologia e segurança da informação especializadas. 4) Serviços especializados de comunicação com imprensa, mídia, clientes e investidores.

iv. **Definir uma estrutura interna de respostas** – Devem ser identificadas pessoas chaves que direcionem a comunicação interna e externa. Outro ponto importante é estabelecer uma estrutura de respostas previamente validada e aprovada para cada público específico, sendo eles, entre outros: 1) Titular dos dados. 2) Autoridade Nacional de Proteção de dados. 3) Mídia especializada. 4) Imprensa. 5) Colaboradores e Fornecedores.

v. **Simulação de incidentes de segurança de dados pessoais** – O objetivo da simulação é validar se os pontos descritos no plano funcionam de fato e quanto tempo leva para mobiliar as pessoas envolvidas, criando uma sala de crise, estabelecer os devidos contatos, criar as comunicações necessárias e no tempo adequado, monitorar a repercussão na mídia e imprensa. A simulação é um importante exercício que ajudar a mensurar e eficiência e eficácia do plano de respostas.

vi. Medidas pós crise – Validar se os dados "expostos" de fato constituem uma base de dados da organização (Controlador ou Operador) e se os dados objetos de tal incidente possuem o enquadramento de "Dados Pessoais/Dados Sensíveis".

vii. Documentação do ocorrido – Elaborar documentação técnica detalhada de como ocorreu tal incidente, quais foram as lições aprendidas, identificar possíveis sistemas que possuem a mesma exposição.

viii. Investigações e coleta de provas digitais – Identificar possível responsável pelo ilícito, bem como comprovar diligência na condução das análises e provas digitais.

viii. Monitoramento em ambiente *Web* e *deep web* – Em casos de vazamento de informações pessoais é importante monitorar redes sociais, *web* e *deep web* em busca de repercussões do incidente, e identificar possíveis "vendas ou negociações" de dados pessoais relacionados ao evento. Existem serviços especializados que podem ser contratados para tal monitoramento.

ANEXO I

Sugestão de Modelo de Termo de Consentimento (Não Vinculativo)

(Controlador dos Dados Pessoais e Informações de contato do Controlador)

Pelo presente termo, autorizo o tratamento dos meus dados pessoais para as finalidades de (listar as finalidades).

Autorizo também o compartilhamento dos meus dados pessoais com empresas do grupo e parceiros comerciais envolvidos na consecução das finalidades acima (se possível, listar as empresas com as quais o compartilhamento é realizado ou os ramos de atividade das mesmas segundo as finalidades listadas acima, ex: agências de viagens, hotéis, empresas de telemarketing, etc.).

(facultativo)

Autorizo a transferência internacional dos meus dados pessoais para as empresas do grupo e parceiros comerciais envolvidos na consecução das finalidades acima, situados notadamente nos seguintes países (citar os países).

Nome e qualificação:

_____, _____ de _____ de 20____.

_____

Assinatura