Manual LGPD

no Iamspe

Governador do Estado
Tarcísio de Freitas

Secretário de Gestão e Governo Digital
Caio Mario Paes de Andrade

Superintendente Iamspe
Maria das Graças Bigal Barboza da Silva

Chefe de Gabinete Iamspe
Vera Lucia Guerrera

Diretoria Iamspe

HSPE - "FMO"
Dr. Marcelo Itiro Takano

Administração
Paulo Sergio Pedrão

Centro de Desenvolvimento de Ensino e Pesquisa (Cedep)
Fabiano Rebouças Ribeiro

Prevenir
Neusa Nakao Sato

Tecnologia da Informação
Ricardo Cezar de Moura Juca

Coordenação Editorial: Gestão de Comunicação Corporativa

Projeto Gráfico: Adriana Rocha

Instituto de Assistência Médica ao Servidor Público Estadual (Iamspe)
Av. Ibirapuera, 981 - V. Clementino - 04029-000 - São Paulo - SP
www.iamspe.sp.gov.br

2023

Índice

INTRODUÇÃO

O Manual Lei Geral de Proteção de Dados (LGPD) no Iamspe é um documento que foi especialmente elaborado para você, profissional que desempenha um papel fundamental na proteção das informações pessoais e confidenciais dos nossos usuários.

Elaborado com base na Lei n° 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), este guia traz conceitos e orientações úteis sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado. São informações que reforçam a importância da privacidade dos dados no contexto de atendimento médico-hospitalar oferecido pelo Iamspe.

Nem seria preciso destacar a importância da privacidade dos dados em um ambiente hospitalar. Do mesmo modo que os pacientes confiam em nós para cuidar de seus problemas de saúde, nós, como profissionais das áreas de saúde e o administrativo, temos a responsabilidade de garantir que as informações pessoais dos usuários sejam tratadas com o mais alto nível de sigilo e proteção.

Além disso, leis e regulamentações rigorosas estão em vigor para garantir a confidencialidade dos dados de saúde. Uma violação de privacidade pode ter consequências sérias, tanto para os pacientes quanto para o Iamspe. Isso inclui não só danos à reputação do Instituto e seus profissionais, mas também consequências legais graves.

Boa leitura!

PRINCIPAIS CONCEITOS

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

- 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.

- Dado pessoal de criança e de adolescente: o Estatuto da Criança e do Adolescente (ECA) considera criança a pessoa até 12 anos de idade incompletos e, adolescente aquela entre 12 e 18 anos de idade. Em especial, a LGPD determina que as informações sobre o tratamento de dados pessoais de crianças e de adolescentes deverão ser fornecidas de maneira simples, clara e acessível de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

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

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

- Controlador: pessoa natural ou jurídica, de direito público ou privado, responsável por decisões sobre tratamento dos dados.

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

- Encarregado de Dados (DPO): 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).

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

- Autoridade nacional: Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

- 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.

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

- Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas 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.

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

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

- Tratamento de dados: toda operação realizada com dados pessoais, como as que se referem ao glossário a seguir:

GLOSSÁRIO

Acesso - possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo etc., visando receber, fornecer, ou eliminar dados

Armazenamento - ação ou resultado de manter ou conservar em repositório um dado

Arquivamento - ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotada a sua vigência

Avaliação - ato ou efeito de calcular valor sobre um ou mais dados

Classificação - modo de ordenar os dados conforme critério estabelecido

Coleta - recolhimento de dados com finalidade específica

Comunicação - transmitir informações pertinentes a políticas de ação sobre os dados

Controle - ação ou poder de regular, determinar ou monitorar ações sobre o dado

Difusão - ato ou efeito de divulgação, propagação, multiplicação dos dados

Distribuição - ato ou efeito de dispor de dados conforme critério estabelecido

Eliminação - ato ou efeito de excluir ou destruir dado do repositório

Extração - ato de copiar ou retirar dados do repositório em que se encontrava

Modificação - ato ou efeito de alteração do dado

Processamento - ato ou efeito de processar dados

Produção - criação de bens e de serviços a partir do tratamento de dados

Recepção - ato de receber os dados ao final da transmissão

Reprodução - cópia de dado preexistente obtido por meio de qualquer processo

Transferência - mudança de dados de uma área de armazenamento para outra, ou para terceiro

Transmissão - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc.

Utilização - ato ou efeito do aproveitamento dos dados

PAPÉIS E RESPONSABILIDADES

Controlador

O controlador, na figura do Iamspe, é o agente responsável por tomar as principais decisões referentes ao tratamento de dados pessoais e por definir a finalidade destes tratamentos. Entre essas decisões, incluem-se as instruções fornecidas a operadores contratados (fornecedores) para a realização de um determinado tratamento de dados pessoais.

A importância prática do conceito acima é justificada pelo fato de a LGPD atribuir obrigações específicas ao controlador como: indicar um Encarregado de Dados, elaborar relatório de impacto à proteção de dados pessoais, comprovar que o consentimento obtido do titular atende às exigências legais, comunicar à ANPD sobre a ocorrência de incidentes de segurança. Além disso, a atribuição de responsabilidades em relação à reparação por danos decorrentes de atos ilícitos é distinta conforme a qualificação do agente de tratamento - controlador ou operador-, conforme o disposto na Lei.

Os direitos dos titulares (art. 18) são exercidos em face do controlador, a quem compete, entre outras providências:

- ✓ Fornecer informações relativas ao tratamento,
- ✓ Assegurar a correção e a eliminação de dados pessoais,
- ✓ Receber requerimento de oposição a tratamento.

O titular dos dados pode ainda peticionar contra o controlador perante a ANPD, o que denota a relevância da compreensão do conceito não só para os profissionais da área, mas também para o cidadão comum.

Encarregado de Dados (DPO)

O Iamspe, por intermédio da Portaria nº 9, de 05 de abril de 2023, designou a servidora Thaisa Lavra como Encarregada de Dados do Iamspe, em conformidade com o art. 8º, do Decreto º 65.347/2020 e art. 41, da Lei nº 13.709/2018 (“LGPD”). O Encarregado de Dados,chamado de DPO, tem várias funções descritas a seguir neste manual:

FUNÇÕES DO ENCARREGADO DE DADOS

I. Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II. Receber comunicações da Autoridade Nacional de Proteção de Dados (ANPD) e adotar providências;

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

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

Comitê de Privacidade

O Comitê de Privacidade é um órgão de governança do Iamspe cujo objetivo principal é auxiliar na implementação e manutenção de práticas adequadas de privacidade de dados, conforme a LGPD e demais orientações normativas. Responsabilidades em destaque:

I. Assessorar o Iamspe na construção e revisão de políticas e procedimentos relacionados à privacidade de dados e segurança da informação;

II. Acompanhar e avaliar os processos de coleta, armazenamento, processamento e compartilhamento de dados pessoais;

III. Identificar e monitorar os riscos e vulnerabilidades e propor medidas técnicas organizacionais para sua mitigação;

IV. Promover treinamentos e ações de conscientização aos colaboradores sobre boas práticas de privacidade de dados;

V. Monitorar o cumprimento das leis de privacidade de dados e recomendar ações corretivas quando necessário;

VI. Atuar como contato nas questões de privacidade de dados, internamente, junto a autoridades reguladoras, e indivíduos afetados;

VII. Manter-se atualizado sobre as mudanças nas leis e regulamentos de privacidade de dados e informar o Iamspe sobre suas implicações legais e regulamentares.

DIREITOS DOS TITULARES

Os direitos dos titulares de dados são fundamentais quando se trata de privacidade e proteção de dados. Aqui estão alguns dos direitos que podem ser exercidos por meio do site Iamspe:

I. Direito ao acesso: Os titulares têm o direito de acessar os dados pessoais que uma organização possui sobre eles e obter informações sobre como esses dados estão sendo processados.

II. Direito de Confirmação: Os titulares têm o direito de serem informados de forma clara e transparente sobre como seus dados pessoais são coletados, usados, compartilhados e armazenados.

III. Direito à retificação: Os titulares têm o direito de solicitar a correção ou atualização de seus dados pessoais caso estejam incorretos, incompletos ou desatualizados.

IV. Direito de Anonimização: Os titulares têm o direito de solicitar que seus dados pessoais sejam anonimizados, desde que não haja uma base legal ou legítima para a retenção desses dados.

V. Informações sobre compartilhamento: Os titulares têm o direito de serem informados sobre com quem seus dados pessoais estão sendo compartilhados. Isso inclui informações sobre terceiros, fornecedores ou outros órgãos públicos com as quais o Iamspe pode compartilhar os dados, além dos fins para os quais esses dados estão sendo compartilhados.

VI. Direito de Eliminação: Os titulares têm o direito de solicitar a exclusão de seus dados pessoais, desde que não haja uma base legal ou legítima para a retenção desses dados.

VII. Revogação de Consentimento: Os titulares têm o direito de revogar o consentimento, não sendo passível de tratamento posterior. Eventuais exceções dependem de análise pontual.

O site do Iamspe concentra informações detalhadas sobre direitos e como exercê-los. O item **Fale com o DPO** é o ambiente para o titular exercer seus direitos junto ao Encarregado de Dados.

Além disso, caso tenha dúvidas, deseje relatar violações de privacidade ou buscar orientações sobre práticas de privacidade e segurança, entre em contato pelo e-mail lgpd@iamspe.sp.gov.br

BOAS PRÁTICAS

Abaixo diretrizes e práticas que os colaboradores devem seguir para proteger a privacidade dos dados sob guarda do Iamspe:

- Manter senhas seguras e não as compartilhar: Os colaboradores devem criar senhas fortes, contendo uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais. Além disso, eles devem evitar compartilhar suas senhas com outras pessoas ou anotá-las em locais facilmente acessíveis.

- Utilizar apenas sistemas autorizados para acessar informações confidenciais: Os colaboradores devem utilizar apenas os sistemas e aplicativos autorizados pelo Iamspe para acessar informações confidenciais de saúde. O acesso não deve ser feito através de dispositivos pessoais ou não autorizados.

- Manter o monitoramento adequado do acesso a registros de saúde: É fundamental que os colaboradores monitorem de perto o acesso aos registros de saúde dos pacientes. Isso inclui verificar regularmente os registros de acesso e garantir que apenas as pessoas autorizadas tenham acesso às informações confidenciais.

- Garantir a devida proteção física e digital dos dados de saúde: Os colaboradores devem proteger adequadamente os dados de saúde tanto em formato físico quanto digital. Isso envolve manter os arquivos físicos trancados em armários seguros quando não estiverem em uso, evitar deixar dispositivos eletrônicos desbloqueados e proteger os computadores com senhas e softwares de segurança atualizados.

- Comunicar imediatamente qualquer incidente de segurança ou violação de privacidade: Caso um colaborador identifique ou suspeite de uma violação de privacidade dos pacientes, deve comunicar à equipe responsável pela segurança da informação ou à pessoa designada. A notificação precoce é essencial para adotar as medidas necessárias e mitigar os danos.

- Participar de treinamentos regulares sobre segurança e privacidade: Os colaboradores devem participar de treinamentos regulares sobre segurança da informação e privacidade. Isso ajuda a manter-se atualizado sobre as melhores práticas, ameaças atuais e mudanças nas políticas e regulamentações relacionadas à proteção de dados de saúde.

- Limitar o acesso às informações confidenciais: Os colaboradores devem ter acesso somente às informações necessárias para realizar suas funções. O acesso deve ser estritamente limitado às informações que são relevantes para o desempenho de suas tarefas e devem evitar acessar ou divulgar informações desnecessárias.

- Criptografar informações confidenciais durante a transmissão: Sempre que informações confidenciais de saúde precisarem ser transmitidas eletronicamente, os colaboradores devem garantir que elas sejam criptografadas para proteger a privacidade dos pacientes durante o trânsito.

- Compartilhamento seguro de informações: Ao compartilhar informações sensíveis por e-mail ou por meio de outros meios eletrônicos, verifique se você está usando métodos seguros, como criptografia ou sistemas seguros de compartilhamento de arquivos.

Dicas para o descarte adequado:

-Ao descartar informações em papel ou dispositivos eletrônicos, certifique-se de fazer isso de forma segura.

-Utilize trituradoras de papel para documentos físicos e utilize softwares especializados para garantir a exclusão segura de dados em dispositivos eletrônicos.

-Folhas com informações de pacientes ou de colaboradores não podem ser jogadas em lixo comum, devem ser trituradas ou incineradas!

-Sempre que possível disponibilizar um lixo lacrado no setor para colocação deste tipo de conteúdo.

- Esteja atento aos sinais de engenharia social: Esteja ciente de tentativas de manipulação, como e-mails ou ligações suspeitas solicitando informações pessoais ou confidenciais de titulares. Além disso, fique alerta para mensagens de phishing que possam tentar enganá-lo para divulgar informações sensíveis ou clicar em links maliciosos, tanto por e-mail, aplicativo de mensagens ou SMS. Essas diretrizes e boas práticas visam promover uma cultura de segurança e privacidade dos dados de saúde, protegendo a confidencialidade e a privacidade dos pacientes.

- Não deixe notas com login e senha ou com informações que possam facilitar o acesso de terceiros em seu equipamento. Mantenha guardado documentos físicos com informações sigilosas e confidenciais.

Atenção aos comportamentos incomuns!

-Esteja atento a atividades suspeitas nos sistemas, como acesso não autorizado a registros de pacientes ou alterações não autorizadas em informações confidenciais.

-Verifique se há sinais de manipulação ou invasão em dispositivos, como computadores ou dispositivos móveis.

-Atente-se às atividades e comportamentos incomuns em seu ambiente de trabalho, como tentativas repetidas de acesso não autorizado, solicitações de informações confidenciais por parte de terceiros desconhecidos ou comportamentos que violem as políticas de segurança.

Ao aderir às diretrizes e boas práticas descritas neste manual, os colaboradores desempenham um papel fundamental na salvaguarda das informações confidenciais e na manutenção da confiança dos pacientes. É essencial que todos estejam cientes dos riscos associados a violações de privacidade e se sintam capacitados para tomar ações apropriadas para prevenir incidentes de segurança.

Anotações


Iamspe
A saúde do Servidor


SÃO
PAULO
GOVERNO
DO ESTADO
Secretaria de
Gestão e
Governo Digital