GUIA LGPD

PARA O SETOR HOSPITALAR

FBH
FEDERAÇÃO BRASILEIRA DE HOSPITAIS

P&B COMPLIANCE | PAGLIA & BREUNIG

GUIA LGPD

PARA O SETOR HOSPITALAR

ORIENTAÇÕES PARA IMPLEMENTAÇÃO DAS ADEQUAÇÕES NECESSÁRIAS À APLICAÇÃO DA NOVA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) EM HOSPITAIS

2020

EXPEDIENTE

DIREÇÃO DE PROJETO

Presidente | Adelvânio Francisco Morato
Superintendente | Luiz Fernando Silva
Advogada | Lidia Hatsumi Yoshikawa

CONSULTORIA EM PROTEÇÃO DE DADOS E DIREÇÃO DE CONTEÚDO

Sócio-fundador | Renato Breunig
Coordenador de Proteção de Dados | Lucas Paglia
Coordenador de *Compliance* | Bruno Ferola

Direção Executiva | Viviã de Sousa
Edição de conteúdo | Felipe Nabuco
Revisão de textos | Amanda Vasconcelos
Projeto gráfico e diagramação | Viva Comunicação Group

GUIA LGPD

PARA O SETOR HOSPITALAR

SOBRE A FBH

A FBH foi criada em 1966 para fornecer representatividade e evolução ao Setor Hospitalar, área fundamental para a promoção do cuidado com as pessoas, e, desde então, vem lutando pela melhoria do segmento.

Com mais de 50 anos de trajetória, a Federação viu de perto a evolução e a luta do segmento, e trabalha ativamente para que o setor se fortaleça e se desenvolva de forma estratégica, qualificada e sustentável. É a legítima representante do Setor Hospitalar e reúne 15 Federadas, que trabalham com o mesmo propósito nos principais estados do país.

Pautada pela ética, pela excelência e pelo compromisso com a Saúde, a FBH atua nas principais áreas para a promoção do desenvolvimento, representando os interesses dos hospitais e prestando suporte aos associados, além de promover informação estratégica e ações estruturadas para qualificar a rede hospitalar privada do país.

A saúde move o país e a FBH cuida dos hospitais, para que os hospitais cuidem da saúde das pessoas!

ATUAÇÃO

- Elaboração de estudos, relatórios e publicações para ampliar o acesso à informação do setor na compreensão de medidas e ações que precisam ser estruturadas para a redução da alta carga tributária;
- Reivindicação do acesso a linhas de créditos mais justas e acessíveis, para que os hospitais continuem gerando empregos, qualificando profissionais, desenvolvendo a economia do segmento e oferecendo um atendimento cada vez mais qualificado e humanizado para todos;
- Articulação como interlocutora das demandas do setor com os Poderes Executivo, Legislativo e Judiciário, para a construção de um novo cenário da Saúde no país, promovendo um debate pautado nas principais discussões em torno de grandes temas nacionais que impactam diretamente o Setor Hospitalar, em especial a carga tributária imposta ao setor, matéria de constante debate da Federação junto ao poder público e ao Congresso Nacional;
- Luta pela mitigação da crise financeira que atinge uma significativa parcela dos hospitais particulares conveniados ou não ao SUS, além do reajuste da tabela dos procedimentos do SUS, que ficou sem qualquer correção de 1994 a 1999, resultando em uma defasagem acentuada e jamais corrigida.

SOBRE A P&B *COMPLIANCE*

Somos um escritório de *Compliance*, com sede na Vila Olímpia, em São Paulo, formado por sócios com especialização no tema pela Fundação Getúlio Vargas de São Paulo (FGV-SP), associado ao Instituto Ethos, conectado com a transformação digital. Prestamos assessoria especializada em:

1. *Compliance* e Ética Corporativa:

- Desenvolvimento de Programas de *Compliance* e treinamentos;
- Avaliação das práticas adotadas para confirmar se estão de acordo com leis, regulamentos e políticas internas;
- *Due Diligence* de *Compliance* Anticorrupção e para investigação de fraudes;
- Consultoria em processos de certificação de integridade e ISO 37001;
- Assistência na avaliação de obrigações contratuais, de governança e de riscos corporativos;
- Suporte na execução das rotinas de Programa de *Compliance*, como treinamentos, comunicações, investigações internas, estruturação de comitês etc.

2. Privacidade e Proteção de Dados:

- Desenvolvimento de programas de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD);
- Avaliação das práticas adotadas para confirmar se estão de acordo com leis, regulamentos e políticas internas, como ISO 27001;
- Treinamentos e consultoria sobre boas práticas nacionais e internacionais;
- Consultoria em processos de adequação para os pilares: Legal, Tecnologia da Informação e Segurança da Informação;
- Assistência na avaliação de obrigações contratuais e de governança corporativa de tratamento de dados;
- Assessoria ao DPO e na avaliação de riscos de vazamento de dados.

Trabalhamos investindo em inovação, sempre com o olhar humano e especializado dos nossos profissionais, e garantimos um atendimento moderno, confiável e eficiente.

ASSOCIAÇÕES FBH

AHEAL – Associação de Hospitais do Estado de Alagoas

AHSEB – Associação de Hospitais e Serviços de Saúde do Estado da Bahia

AHECE – Associação de Hospitais do Estado do Ceará

AHCES – Associação de Hospitais, Clínicas e Prestadores de Serviços Afins à Área de Saúde do Espírito Santo

AHEG – Associação de Hospitais do Estado de Goiás

AHMG – Associação de Hospitais de Minas Gerais

AHCSEP – Associação de Hospitais e Casas de Saúde do Estado do Pará

APH – Associação Paraibana de Hospitais

AHOPAR – Associação de Hospitais do Estado do Paraná

ANH – Associação Nordestina de Hospitais

AHERJ – Associação de Hospitais do Estado do Rio de Janeiro

AHORN – Associação de Hospitais do Estado do Rio Grande do Norte

AHRGS – Associação de Hospitais e Estabelecimento de Saúde do Rio Grande do Sul

AHESC – Associação de Hospitais do Estado de Santa Catarina

AHESP – Associação de Hospitais do Estado de São Paulo

SUMÁRIO

SUMÁRIO


PALAVRA

PALAVRA DO PRESIDENTE

Adelvânio Francisco Morato
Presidente da FBH

A LGPD impõe boas práticas de governança e controle na gestão hospitalar para a proteção das informações que são coletadas cotidianamente no ambiente de trabalho.

A aplicação das normas da Lei Geral de Proteção de Dados (LGPD) já é uma realidade, e o grande desafio que se apresenta para os hospitais privados é a obtenção da segurança jurídica nas relações que mantém com pessoas físicas e jurídicas, necessária para a continuidade das suas atividades essenciais de saúde.

A Federação Brasileira de Hospitais (FBH), entidade pioneira na representação dos estabelecimentos privados e principal indutora da política de qualificação da rede hospitalar brasileira, tem a satisfação de apresentar esta publicação como uma forma de contribuir à imprescindível tarefa que os hospitais terão de se adequar à nova legislação.

Importante evidenciar que a adequação à nova LGPD é necessária e salvaguarda a segurança jurídica de todos os atores envolvidos no tratamento da informação: o hospital, o paciente, o profissional e o plano de saúde. A nova legislação está fundamentada em um conjunto de princípios e conceitos que a permite se adaptar ao dinamismo e à velocidade com que o mundo digital se transforma.

Na medida em que as atividades humanas passam a ser, cada vez mais, potencializadas pela mediação de tecnologias digitais, há uma exigência natural da sociedade para que essas relações levem em consideração a privacidade e a proteção dos dados pessoais em todos os âmbitos. A responsabilidade sobre o Setor Saúde se sobressai, sobretudo por ser aquele que mais trata de dados pessoais sensíveis – um dos focos primordiais da nova Lei.

A LGPD impõe boas práticas de governança e controle na gestão hospitalar para a proteção das informações que são coletadas, cotidianamente, no ambiente de trabalho. Nesta publicação, você encontrará as orientações para elaboração de um programa de governança em proteção de dados, bem como para criação de um comitê responsável pela aplicação deste programa. Também terá noções sobre mapeamento dos dados tratados, análise de riscos, proteção e monitoramento das novidades/tecnologias sobre o tema. Vale recomendar aqui a leitura da Nota Técnica nº 3/2019/GEPIN/DIRAD-DIDES/DIDES, da Agência Nacional de Saúde Suplementar (ANS) (BRASIL, 2019).

Cabe lembrar que, mais que adaptação, a LGPD exige uma transformação da cultura organizacional em defesa do direito à privacidade, sob pena de pesadas sanções aos hospitais. Portanto, será necessário às gestões hospitalares, também, estabelecer rotinas de treinamentos e atividades estratégicas de comunicação, a fim de obter conscientização e engajamento de seus colaboradores.

Para construir esse precioso projeto, fomos atrás de quem tem expertise e muito conhecimento no mercado para compartilhar sobre o tema. Nosso sincero agradecimento à P&B Consultoria, por nos auxiliar nesta tarefa de adequar nossos hospitais à LGPD e em ações de conscientização sobre a cultura de privacidade e proteção de dados no país.

Cabe lembrar que a LGPD exige a transformação da cultura organizacional de forma a garantir o direito à privacidade, sob pena de pesadas sanções aos hospitais.

1. CONCEITO DE PRIVACIDADE

A proteção à privacidade é essencial para o ser humano: todos temos direito a não sermos incomodados, a termos nossas comunicações livres de interferência e ao sigilo das informações.

Antigamente, a questão da privacidade associava-se à busca por alguma forma de isolamento, refúgio ou segredo, o chamado "direito de estar só". A partir da revolução tecnológica, porém, tal conceito tornou-se mais abrangente, passando a relacionar-se a outros escopos, como a procura por igualdade, liberdade de escolha, vontade de não ser discriminado e até mesmo ao desenvolvimento da personalidade. Em suma, pode-se afirmar que a proteção à privacidade é essencial para o ser humano: todos temos direito a não sermos incomodados, a termos nossas comunicações livres de interferência e ao sigilo das informações.

Nesse sentido, é correto afirmar que cada vez mais o fornecimento de dados realizado pelos próprios indivíduos, seja às empresas privadas (como planos de saúde e redes sociais), seja aos órgãos públicos (como a declaração de Imposto de Renda), abre margem para diversas formas de tratamento, possibilitando a identificação dessas pessoas sem o seu devido conhecimento. Estas informações são estruturadas em grandes bancos de dados e consideradas como o principal fator em uma avaliação de crédito, na aprovação de um plano de saúde, na obtenção de um emprego, na passagem pela migração em um país estrangeiro e em inúmeras outras situações.

O acúmulo de informações pode ser, também, uma grande fonte de renda para empresas privadas, que se utilizam do banco de dados para traçar hábitos de consumo, indicativos de personalidade e até mesmo informações íntimas de caráter privado de milhares de pessoas, vendendo-os para outras empresas com finalidades diversas, bem como a divulgação de produtos por *e-mails* ou por mensagens de texto.

Sob essa lógica, a Constituição Federal de 1988 estabelece, em seu Art. 5º, incisos X e XII (BRASIL, 1988), o direito à proteção à intimidade, assim como a inviolabilidade do sigilo de correspondências e das comunicações, protegendo, portanto, diversos aspectos que asseguram a privacidade dos cidadãos brasileiros. Contudo, ainda que exista tal previsão, é indiscutível que a vida em sociedade pressupõe o compartilhamento de informações, sendo, desse modo, necessária a compatibilização do direito à privacidade com a necessidade de circulação de dados. Tal processo se dá mediante a operação de atos regulatórios, que possibilitam aos cidadãos um efetivo controle de suas informações pessoais.

2

2. A LEI GERAL DE PROTEÇÃO DE DADOS NO AMBIENTE HOSPITALAR

Além de armazenar e cuidar dos dados dos pacientes, é dever da instituição informar ao público a razão que justifica a coleta de seus dados.

A LGPD, responsável por melhor regulamentar o tratamento cedido a dados pessoais no território nacional, impactou de maneira significativa a atuação dos hospitais, em especial no que diz respeito à relação entre paciente e instituição.

Como sabido, as instituições hospitalares necessitam de informações e dados de pacientes para atuarem de maneira adequada. O tratamento destes dados, a partir da sanção da Lei, deve ocorrer em conformidade com alguns parâmetros específicos e, em se tratando dos dados relativos à saúde, receber tratamento peculiar, haja vista que os últimos são classificados como dados sensíveis pela LGPD.

Dados relativos à saúde, nos termos do Art. 4º da Lei (BRASIL, 2018), são aqueles relacionados com a saúde física ou mental de uma pessoa natural, incluindo a prestação de serviços, que revelem informações sobre o seu estado de saúde. Estes, assim como os demais dados sensíveis dispostos no texto legal, recebem uma proteção mais ampla, exigindo o consentimento explícito dos pacientes e uma finalidade específica – salvo em hipóteses excepcionais que os dispensem, como em casos de preservação da vida ou da integridade física.

A gestão do consentimento integra uma das bases legais[1] mais importantes previstas pela LGPD. A organização hospitalar é encarregada de fornecer uma interface para que o indivíduo possa autorizar, bloquear ou revogar o consentimento para o tratamento de dados pessoais a qualquer momento. No mais, é obrigatório que haja, à disposição dos pacientes, uma maneira fácil de revogar o seu consentimento e, ainda, que a instituição tenha um controle e um armazenamento de documentos relativos a ele (digitais ou físicos).

[1] Ver Apêndice desta publicação.

Retomando a noção de que os dados relativos à saúde devem ser obtidos em decorrência de uma finalidade específica, além de armazenar e cuidar dos dados dos pacientes, é dever da instituição informar ao público a razão que justifica a coleta de seus dados – o que, por conseguinte, evidencia a necessidade da devida conscientização de todos os funcionários do hospital para que sejam capazes de esclarecer eventuais dúvidas sobre a exigência de coleta daquelas informações.

A LGPD exige que as organizações tenham uma política clara e transparente para a coleta e o tratamento de dados, que deve ser amplamente divulgada para seus colaboradores e, também, para os titulares de seus dados. A conscientização – que, além dos funcionários, deve abranger os colaboradores e os parceiros – pode ser feita por meio de palestras, apresentações, videoconferências e até mesmo com pequenos informes enviados aos funcionários de tempos em tempos.

O compartilhamento de dados pode, muitas vezes, apresentar grande risco, pois as pessoas, mediante a exposição de elementos sensíveis sobre si mesmas ou sobre familiares, possibilitam que tais informações sejam utilizadas para práticas ilícitas, como fraudes e crimes – no mundo digital ou não. A cultura de proteção de dados, nesse contexto, há de ser urgentemente difundida, a fim de proteger a grande maioria da população que, alheia aos riscos inerentes ao compartilhamento, expõe-se demasiadamente (seja em suas redes sociais, seja realizando cadastros para receber descontos ou brindes).

A LGPD exige que as organizações tenham uma política clara e transparente para a coleta e o tratamento de dados, que deve ser amplamente divulgada para seus colaboradores e, também, para os titulares de seus dados.

3

3. CONCEITOS LEGAIS DA LEI GERAL DE PROTEÇÃO DE DADOS

3.1. PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS

A LGPD possui dez princípios, além da boa-fé, que devem ser observados por todos aqueles que tratarem dados pessoais. São eles:

(i) **Finalidade**: simboliza que as finalidades para o tratamento dos dados pessoais devem ser legítimas, específicas, explícitas e informadas ao titular;

(ii) **Adequação**: significa que as atividades devem ser condizentes com a destinação para a qual os dados pessoais foram coletados;

(iii) **Necessidade**: implica a coleta da menor quantidade possível de dados pessoais para cada atividade;

(iv) **Livre acesso**: possibilita que os titulares tenham acesso de forma fácil à consulta sobre os seus dados pessoais que estejam sendo tratados;

(v) **Qualidade dos dados pessoais:** assegura aos titulares o direito de que os dados pessoais estejam corretos e atualizados;

(vi) **Transparência**: garante aos titulares que as informações sobre as atividades de tratamento de dados pessoais estejam em linguagem clara e simples;

(vii) **Segurança**: obriga os agentes de tratamento de dados pessoais a se utilizarem de medidas técnicas e administrativas aptas a proteger estes dados;

(viii) **Prevenção**: obriga os agentes de tratamento de dados pessoais a adotarem medidas para prevenir a ocorrência de danos em virtude do tratamento;

(ix) **Não discriminação**: impossibilita o tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos;

(x) **Responsabilização e prestação de contas**: os agentes de tratamento de dados pessoais devem adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção aos dados pessoais, atestando, inclusive, a eficácia dessas medidas.

3.2. DIREITO DOS TITULARES

Inicialmente, a LGPD informa que toda pessoa natural tem assegurados e garantidos os seus direitos fundamentais de liberdade, intimidade e privacidade, o que é essencial, pois, como vimos no início desta cartilha, a proteção de dados visa complementá-los.

Outros direitos garantidos ao titular de dados pessoais são:

(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 Lei;

(v) Portabilidade dos dados pessoais (ou seja, a transferência dos dados pessoais de um controlador a outro, desde que assegurados os segredos industrial e comercial);

(vi) Eliminação dos dados pessoais tratados sob a base legal do consentimento;

(vii) Informações sobre o compartilhamento de dados pessoais;

(viii) Informações sobre a possibilidade de não fornecer o consentimento e sobre as consequências de tal conduta;

(ix) Revogação do consentimento.

3.3. COMUNICAÇÕES COM A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E COM OS TITULARES DE DADOS PESSOAIS

As pessoas jurídicas deverão indicar um encarregado pelo tratamento de dados pessoais, que terá a função de se comunicar com a Autoridade Nacional de Proteção de Dados (ANPD) e com os titulares de dados pessoais, prestando informações quando solicitadas a respeito das atividades de tratamento de dados pessoais realizadas. Incumbe à ANPD, também, regulamentar diversos pontos sobre a LGPD e fiscalizar o cumprimento da legislação.

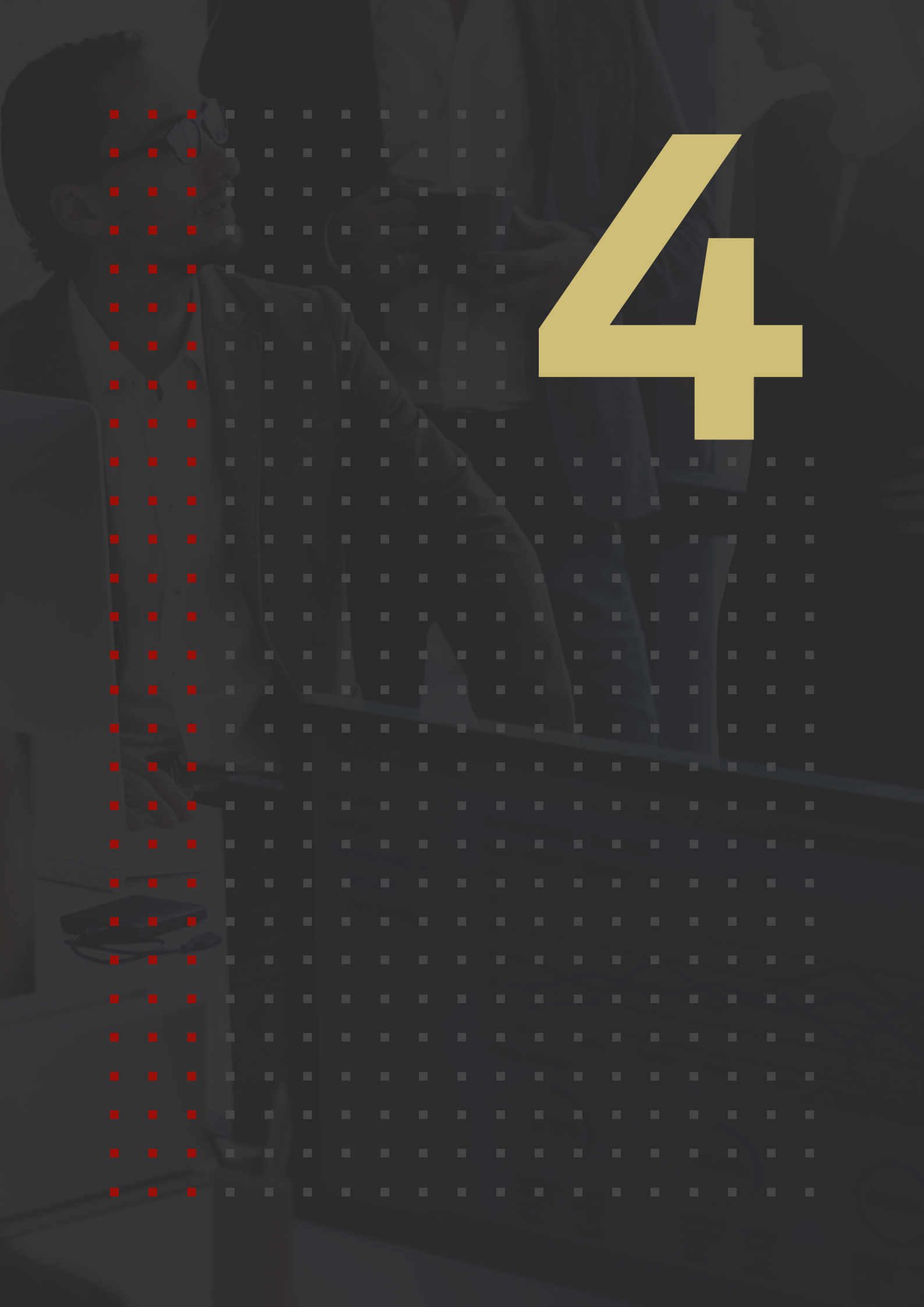
3.4. OBRIGAÇÕES E RESPONSABILIDADES

A LGPD, além de diferenciar os agentes de tratamento, dispõe sobre as obrigações e as responsabilidades no caso de danos decorrentes do tratamento inadequado de dados pessoais e de incidentes relativos à segurança da informação.

A principal obrigação dos agentes acima citados é, de acordo com a Lei, que mantenham um registro das operações de tratamento que realizarem, especialmente quando este tratamento de dados pessoais ocorrer segundo a base legal do legítimo interesse.

No que diz respeito especificamente à atuação do operador, este deverá realizar o tratamento de dados pessoais conforme as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. É necessário que todas as instruções sejam claras e, preferencialmente, formais, para que não haja incerteza ou falha no processo de tratamento de dados pessoais.

O agente de tratamento que, em razão do tratamento inadequado de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. Nesse sentido, o operador, apesar de tratar os dados conforme as instruções fornecidas pelo controlador, também poderá ser responsabilizado e compelido a reparar o dano causado.



4

4. COMO SE ADEQUAR À LEI GERAL DE PROTEÇÃO DE DADOS

O objetivo desta publicação é auxiliar as gestões hospitalares na tarefa de adequar o funcionamento do estabelecimento às novas exigências da LGPD. A seguir, estão elencadas as etapas para consolidação desse projeto de adequação, que prevê:

4.1. PROGRAMA DE GOVERNANÇA EM PROTEÇÃO DE DADOS

Para garantir o efetivo cumprimento das normas, o Art. 50 da LGPD estipula um capítulo exigindo que:

> sejam formuladas regras sobre boas práticas e governança, que estabeleçam as condições, o regime de funcionamento, os procedimentos incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos agentes envolvidos no tratamento dos dados pessoais, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (BRASIL, 2018).

Cada política, norma e ação criada dentro da instituição deve ser documentada, de modo a demonstrar a efetividade de seu programa de governança quando houver questionamento e, em especial, a pedido da ANPD. A adoção de tais políticas não apenas auxilia o cumprimento das obrigações estabelecidas pela Lei, como demonstra os esforços nesse sentido, e todos os registros documentados das ações adotadas serão considerados em uma eventual aplicação de sanção por tratamento inadequado de dados pessoais.

Além disso, mesmo que já exista um conjunto de políticas do hospital, é importante garantir que elas estejam de acordo com a nova Lei: devem estar incluídas no seu conjunto de políticas todas aquelas referentes à segurança da informação, à privacidade, à classificação da informação e ao controle de acesso.

4.2. ESTRUTURAÇÃO DE UM COMITÊ/DEPARTAMENTO DE PROTEÇÃO DE DADOS

Para a correta adequação à LGPD, é essencial que o agente de tratamento estruture um comitê responsável pelo projeto. É fundamental que, neste comitê, estejam presentes e engajadas pessoas da Alta Diretoria do hospital, bem como pessoas de setores que tratam dados pessoais em seu dia a dia, como funcionários dos Recursos Humanos, do *Marketing*, do Jurídico e do *Compliance*.

Os colaboradores da instituição devem ser instruídos de modo a assinarem termo de responsabilidade para que, havendo algum incidente, não seja possível eventual alegação no sentido de desconhecimento das normas e dos procedimentos de segurança da informação do ambiente hospitalar.

4.2.1. Agentes de tratamento

A LGPD estabelece como agentes de tratamento os indivíduos encarregados de controlar ou tratar as informações que contenham dados pessoais. São eles:

a) **Controlador**: a pessoa física ou jurídica que determina como todo e qualquer tratamento de dados pessoais ocorrerá;

b) **Operador**: a pessoa física ou jurídica que segue as determinações vindas do controlador para elaborar o tratamento de dados pessoais.

Em suma, a diferença entre o controlador e o operador reside no escopo da função: o primeiro é responsável pela coleta dos dados pessoais dos titulares, enquanto ao segundo cabe a realização do tratamento destes dados em virtude de contrato, respeitando as instruções do controlador.

Embora a Lei não o defina como agente de tratamento, vale destacar a figura do encarregado, pessoa indicada pelos agentes de tratamento para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

4.3. AVALIAÇÃO E CONSCIENTIZAÇÃO

Como previamente mencionado, a eficácia do programa de adequação à LGPD exige a devida conscientização de todos os profissionais que trabalham dentro do hospital, bem como de eventuais colaboradores. A cultura de proteção de dados deve, impreterivelmente, ser amplamente difundida, haja vista que o programa somente existe com a participação de todos.

Deve-se, nesse contexto, levar em consideração o quanto de informação sobre o projeto os funcionários possuem e, a partir desse ponto, conscientizá-los acerca do objetivo do projeto,

bem como sua estruturação. A instituição deve se familiarizar com a LGPD, com a metodologia do projeto, e entender que todas as atividades serão averiguadas.

4.4. MAPEAMENTO

A LGPD determina que o controlador e o operador mantenham registro das operações de tratamento de dados pessoais que realizarem, desde a etapa de mapeamento de processos, momento de grande importância para a adequação da empresa.

Nesta ocasião, será possível: (i) detalhar cada dado pessoal tratado, entendendo as fases do seu ciclo de vida; (ii) perceber como estes dados são recebidos, de que forma e onde estão armazenados, quem tem acesso e se são compartilhados com terceiros; e, ainda, (iii) analisar seus riscos associados a cada operação, bem como a base legal adequada.

Em suma, é fundamental que todo processo hospitalar que envolva uso de dados pessoais seja mapeado. Essa atividade não só colabora com a identificação dos riscos, como auxilia na minimização da coleta, garantindo que as informações obtidas sejam somente aquelas necessárias para cumprir com sua finalidade.

4.5. ANÁLISE DE GAPS, PLANEJAMENTO E IMPLEMENTAÇÃO

Após o mapeamento dos processos, será possível identificar diversas questões em desacordo com a LGPD ou com as melhores práticas de segurança da informação, ou, ainda, com as práticas setoriais aplicáveis. Neste momento, deve-se definir as bases legais adequadas para cada atividade de tratamento de dados pessoais executadas na instituição, bem como elaborar um relatório com os principais *gaps*, apontando quais são as medidas necessárias para a mitigação de riscos envolvendo incidentes de segurança da informação.

Analisados os *gaps*, será necessário verificar quais são as prioridades da empresa, assim como elaborar um cronograma para mitigar os riscos localizados nas etapas anteriores. No mais, deve haver a indicação de responsáveis para cada atividade de tratamento com necessidade de alteração e a verificação dos diferentes níveis de criticidade de cada medida.

Por último, é chegada a hora de adequar as medidas em desconformidade com a legislação. Neste momento, é imprescindível adequar plataformas, processos, contratos, práticas e documentos que versem sobre o tratamento de dados pessoais.

4.6. PROTEÇÃO

Uma alternativa viável, que exclui a possibilidade de acesso indevido dos dados, é a criptografia. Ela, além de ser evidentemente mais segura, impede, em caso de vazamento, que os dados consigam ser interpretados, evitando que mesmo profissionais com acesso privilegiado alcancem o conteúdo.

Aliás, é bastante recomendado que a instituição invista em equipamentos com bases de proteção atualizadas constantemente, com especial importância em um ambiente crítico como o hospital. Novas formas de ataque surgem periodicamente, e é preciso criar proteção contra elas dentro dos sistemas, além de garantir a disponibilidade de manutenção até mesmo em horários não comerciais ou aos fins de semana.

4.7. MONITORAMENTO

Depois de finalizada a etapa de implementação, encerra-se o projeto de adequação à LGPD. Entretanto, é impossível afirmar que projetos desse tipo, de fato, chegam a um fim definitivo, pois a organização deve, de modo constante, avaliar se está de acordo com a legislação de proteção de dados pessoais. A própria legislação é mutável no que tange à alteração e à regulamentação, o que mostra que a empresa precisará se adequar às novidades no cenário da privacidade.

Dessa maneira, é essencial que a instituição tenha funcionários (internos, externos ou mesmo uma equipe híbrida) capazes de monitorar todas as novidades ocorridas, garantindo, assim, que a organização nunca esteja desatualizada ou sofra alguma sanção eventualmente imposta pela ANPD.

Outro ponto fundamental do monitoramento é a necessidade de treinamentos com certa periodicidade, para que a cultura da proteção aos dados pessoais seja parte do dia a dia do hospital.

Confira os oito passos para se adequar à LGPD:

1

PROGRAMA DE GOVERNANÇA EM PROTEÇÃO DE DADOS

Elaboração de um programa de governança em proteção de dados pessoais, somado à disseminação da cultura e dos valores sobre seu tratamento adequado.

2

ESTRUTURAÇÃO DE UM COMITÊ DE PROTEÇÃO DE DADOS

Estruturação de um comitê responsável pela adequação dos hospitais à LGPD, em que devem estar presentes membros da Alta Diretoria e pessoas que tratem os dados pessoais.

3

AVALIAÇÃO E CONSCIENTIZAÇÃO

Conscientizar os empregados em relação ao objetivo do processo, bem como sua estruturação, mediante palestras, *workshops*, apresentações, vídeoconferências etc.

4

ESTRUTURAÇÃO DE UM COMITÊ DE PROTEÇÃO DE DADOS

Esta etapa busca demonstrar o caminho percorrido pelos dados dentro dos hospitais, desde a sua coleta até o seu descarte. Deve-se analisar a finalidade para qual dado pessoal é tratado, bem como sua base legal e acesso de terceiros.

5

ANÁLISE DE *GAPS*

Nesta etapa, elabora-se um relatório de adequação, que contemple os principais pontos em desacordo com a LGPD e as medidas necessárias para a mitigação de riscos.

6

PLANEJAMENTO

Análise das prioridades dos hospitais em elaborar um cronograma para mitigar os riscos encontrados.

7

IMPLEMENTAÇÃO

Implementação das medidas localizadas no cronograma mediante adequação de plataformas, processos, contratos, práticas e documentos que versem sobre o tratamento de dados pessoais.

8

MONITORAMENTO

Análise de novos projetos, produtos e processos. A organização deve, constantemente, avaliar se suas práticas estão de acordo com a legislação referente à proteção de dados pessoais.

5

5. COMO SE PROTEGER NO AMBIENTE REMOTO

A prática das reuniões de telemedicina, especialmente no atual contexto pandêmico da Covid-19, tornou-se indispensável para o bom funcionamento de hospitais, clínicas e postos de emergência. Esse panorama, porém, exige grande cuidado na realização das consultas, uma vez que, durante tais encontros, pode ocorrer o vazamento de informações sigilosas, exposições indevidas e incidentes de segurança da informação.

É fundamental, portanto, que os funcionários da instituição sejam treinados para a realização de videoconferências – de modo a minimizar os possíveis danos – e instruídos a respeito do funcionamento da plataforma, das regras de conduta e demais informações que sejam relevantes.

Por isso, seguem algumas dicas para se proteger:

5.1 MINIMIZAÇÃO DE EXPOSIÇÕES PESSOAIS

Escolha do ambiente ideal

É importante estar atento ao ambiente físico em que você participará da reunião, principalmente dentro do espaço doméstico. Escolha um local que não tenha grande circulação e, se possível, feche a porta. É comum que vídeos viralizem pela internet com participações inusitadas em videoconferências, como animais de estimação e crianças.

Comporte-se

Embora a reunião possa acontecer em espaço doméstico e descontraído, é fundamental que a etiqueta e o comportamento sejam mantidos exatamente como se você estivesse em ambiente profissional. Portanto, vista-se de acordo com o esperado, arrume os cabelos, lave o rosto, tenha um bloco de anotações à mão e, se possível, indique o momento em que gostaria de participar, sem interromper os demais participantes. A pontualidade também é um fator fundamental para o sucesso da reunião.

Visando ao cumprimento de tais medida por todos os participantes da consulta, recomenda-se um *disclaimer* no convite da reunião, isto é, um pequeno manual de como as pessoas devem se comportar durante a videoconferência, bem como o assunto que será abordado.

Uso de câmeras e microfones

Caso não haja necessidade, deixe a câmera e o microfone desligados para que ocorra menos interrupções durante a reunião. Além disso, recomenda-se a utilização de fones de ouvido com microfone, uma vez que o captador de áudio interno do *notebook* pode causar ecos e distorções. Por fim, prefira áudio ao vídeo, pois, se a qualidade da conexão for baixa, a experiência da reunião poderá ser comprometida.

5.2 SEGURANÇA DA INFORMAÇÃO

Utilize ferramentas confiáveis e, se possível, criptografadas

É importante que o mediador da consulta pesquise previamente todas as ferramentas disponíveis e veja a que melhor se adeque às necessidades de sua reunião, de modo que toda a organização utilize o mesmo sistema, garantindo, assim, que o uso seja coerente e bem manuseado. Ainda, são recomendadas ferramentas com sala de bate-papo criptografada, a fim de que as informações não sejam acessadas de forma indevida ou, em caso de vazamento, não consigam ser interpretadas. Assim, evita-se que os profissionais com acesso privilegiado para a administração da base acessem o conteúdo.

Além disso, forneça um *e-mail* e uma senha para cada usuário acessar a consulta. Esta é uma medida fundamental que garante que só acessarão a reunião e as informações disponibilizadas os funcionários que precisem de tais informações.

Proíba que funcionários gravem as reuniões

Seguindo a linha da segurança da informação, é essencial que os funcionários sejam avisados quanto à permissão ou não da gravação das reuniões. Durante as videoconferências, podem ser expostas informações valiosas sobre a instituição, sobre funcionários e demais ativos de informação. Se possível, utilize aplicativos que não permitam gravações de tela ou registros de imagens (*screenshots*).

5.3 VAZAMENTO DE DADOS PESSOAIS

Fique atento às permissões concedidas aos aplicativos

É essencial que a organização escolha um aplicativo confiável para as videoconferências, conforme destacado acima. Entretanto, os funcionários devem prestar muita atenção às permissões que concedem aos aplicativos, principalmente quando baixados no celular. Suspeite de permissões invasivas e confira os dados aos quais o aplicativo requer acesso para funcionar – os últimos, vale destacar, devem ser relacionados apenas ao funcionamento da câmera e do microfone do aparelho celular.

Desative notificações em *pop-up* ao compartilhar a tela

Ao compartilhar a tela do computador ou do celular durante chamadas de vídeo, é importante desativar notificações em *pop-up* de *e-mails*, redes sociais e aplicativos de mensagens. As mensagens podem tratar de assuntos privados desnecessários à reunião.

Envie o convite da chamada apenas para *e-mails* confiáveis

Não compartilhe *links* de convites de chamadas de vídeo pelas redes sociais. Prefira encaminhá-los de forma privada utilizando o endereço de *e-mail* dos participantes da reunião. Compartilhar a URL dos convites pode atrair desconhecidos e cibercriminosos para a chamada de vídeo, comprometendo informações dos participantes.

Evite o *phishing*

Phishing é um tipo de crime virtual que consiste em coletar informações e dados secretos dos usuários por meio de informações falsas ou dados não reais, porém, muito atrativos. Atualmente, muitos cibercriminosos utilizam *sites* semelhantes àqueles utilizados pelos aplicativos de conferência para "roubar" *logins* e senhas de *e-mails* e fazer mau uso de tais informações. Portanto, é importante estar atento aos *sites* e aos aplicativos que solicitam dados para acesso.

Atualize o antivírus

O antivírus é um programa de segurança básico e essencial. Além de proteger a máquina e os sistemas contra vírus e malwares, também pode evitar travamentos e a lentidão do computador.

REFERÊNCIAS

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Senado Federal, 1988.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 16 nov. 2020.

BRASIL. Agência Nacional de Saúde Suplementar. **Nota Técnica nº 3/2019/GEPIN/DIRAD-DIDES/DIDES**. Brasília: ANS, 2019. Disponível em: https://www.sbac.org.br/wp-content/uploads/2019/12/Nota-Te%CC%81cnica-sobre-LGPD.pdf. Acesso em: 16 nov. 2020.

GLOSSÁRIO

Agente de tratamento: qualquer pessoa, natural ou jurídica, que realize tratamento de dado pessoal.

Anonimização: é o processo técnico que visa, de forma irreversível, retirar a possibilidade de o dado pessoal identificar uma pessoa natural.

Autoridade Nacional de Proteção de Dados (ANPD): é a autoridade criada para oferecer as diretrizes de regulamentação e fiscalização de cumprimento da LGPD mediante a promoção de ações educativas, além da aplicação de sanções e multas. É responsável, ainda, por dirimir as dúvidas quanto ao tratamento de dados pessoais em situações concretas.

Banco de dados/*data center*: qualquer conjunto estruturado, físico, digital ou em nuvem que contenha dado pessoal.

Bases legais: autorização prevista pela LGPD para que o tratamento de dados pessoais seja realizado.

Compartilhamento: ocorre quando dados pessoais são enviados para terceiros. A possibilidade desta prática deve ser expressamente informada ao titular de dados pessoais no momento de sua coleta, uma vez que há, também, uma extensão de responsabilidades entre as partes.

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

> **Manifestação livre:** expressa a genuína vontade de seu titular, que não pode ser pressionado a consentir.
>
> **Manifestação informada:** o titular deve ser informado previamente, de forma completa e detalhada, sobre o tratamento de seus dados pessoais, incluindo natureza, objetivos, métodos, duração, justificativa, finalidades, riscos e benefícios.
>
> **Manifestação inequívoca:** refere-se à manifestação livre de dúvidas ou ambiguidades por parte do titular.

Controlador: o agente de tratamento que determina como todo e qualquer tratamento de dados pessoais ocorrerá.

Dado anonimizado: é o dado pessoal que passou por processo de anonimização e, portanto, não pode mais identificar uma pessoa natural.

Dado pessoal: são quaisquer informações que identificam ou possam identificar uma pessoa natural, de acordo com a LGPD.

> **Dados que identificam uma pessoa natural:** exemplifica-se por *e-mail*, endereço, números de RG e CPF.
>
> **Dados que possam identificar uma pessoa natural:** conjunto de informações que, quando somadas, identificam uma pessoa, como a soma do primeiro nome ao endereço e/ou a características físicas da pessoa natural.

Dado pessoal sensível: são todos os dados pessoais que possam identificar a origem racial ou étnica do usuário, bem como suas convicções religiosas ou políticas, filiação a sindicato ou organização de caráter religioso, filosófico ou político. Contempla, ainda, quando vinculados à pessoa natural, os dados referentes à saúde ou à vida sexual, assim como os dados genéticos ou biométricos. Vale ressaltar que a LGPD estabelece um rol limitado de informações que podem ser enquadradas como sensíveis.

Documento físico e documento digital: os documentos físicos são aqueles elaborados em suportes físicos, por exemplo, em papel. Os documentos digitais, por sua vez, são aqueles elaborados em suportes digitais, localizados em ambiente virtual.

Encarregado: é o responsável por atuar na comunicação entre o controlador, os titulares dos dados e a ANPD. Tem, também, o papel de disseminar a cultura da proteção dos dados pessoais dentro de uma organização e avaliar as atividades de tratamento que ela realiza.

Lei Geral de Proteção de Dados (LGPD): nomenclatura adotada pela Lei Federal nº 13.709/2018, que tem por objetivo assegurar o direito à privacidade e à proteção de dados pessoais, em suportes fáticos ou digitais, mediante tratamento transparente, justificado e seguro. A administração destes dados pode ser realizada por pessoa natural ou jurídica, de direito público ou privado, independentemente da localização de seu titular, desde que alguma parte do processo de tratamento seja realizada em território brasileiro. Busca-se, portanto, proteger os direitos fundamentais de liberdade e privacidade, bem como o de livre desenvolvimento da personalidade da pessoa natural. É importante ressaltar, ainda, que a LGPD não se aplica a qualquer tipo de dado ou informação, apenas a dados pessoais.

Operador: agente de tratamento que segue as determinações do controlador para o tratamento de dados pessoais.

Pessoa jurídica: conjunto de pessoas naturais reunidas em prol do mesmo objetivo ou finalidade sob respaldo jurídico, seja para a prestação de serviços, seja para a comercialização de produtos. A partir do momento de sua criação, a pessoa jurídica adquire personalidade e capacidade própria, e, assim, seus integrantes passam a tomar decisões em nome da pessoa jurídica.

Pessoa natural: todos os seres humanos, independentemente de idade, sexo, nacionalidade, etnia, saúde ou quaisquer outras características, possuindo direitos e obrigações.

Pseudonimização: difere-se da anonimização, pois permite a reversão para que o dado pessoal ocultado volte a identificar uma pessoa natural.

Relatório de Impacto à Proteção de Dados Pessoais (RIPD): documentação elaborada pelo controlador que contemple a descrição completa dos processos de tratamento de dados pessoais, quando este representar risco à liberdade civil e aos direitos fundamentais do titular.

Titular de dados pessoais: a pessoa natural a quem pertence o dado pessoal.

Transferência internacional: quando os dados pessoais são transferidos para empresa terceira ou do mesmo grupo econômico localizado fora do país ou armazenados em servidores de empresas estrangeiras.

Tratamento: toda e qualquer operação realizada com dados pessoais, sendo coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

APÊNDICE

BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS

Para que uma atividade de tratamento de dados pessoais seja realizada, é necessário saber sob qual fundamento de legalidade esta atividade está baseada. A LGPD afirma que, para todo tratamento de dados pessoais, deve haver uma norma legal que o fundamente. A seguir estão as bases legais expostas na Lei:

(i) Para o cumprimento de uma obrigação legal ou regulatória: quando a empresa for obrigada a realizar uma atividade de tratamento de dados pessoais objeto de lei ou regulamentação;

(ii) Realização de estudos por órgão de pesquisa: somente órgãos de pesquisa poderão usar essa base legal para tratar dados pessoais. O tratamento deve ser utilizado para fins de pesquisa e estudos, devendo, sempre que possível, anonimizar dados pessoais;

(iii) Execução de contratos em que o titular seja parte: quando o titular de dados pessoais celebrar um contrato ou mesmo em procedimentos preliminares à celebração de um contrato;

(iv) Exercício regular de direitos em processo judicial, administrativo ou arbitral: quando a empresa ajuizar uma ação em face de um cidadão, seus dados pessoais poderão ser tratados sem que isso represente uma violação;

(v) Proteção da vida ou da incolumidade física do titular ou de terceiro: esta é uma base legal muito importante, pois permite o tratamento de dados pessoais quando um titular estiver em risco de vida. Por exemplo: quando um cidadão é levado a um hospital após sofrer um grave acidente;

(vi) Para a tutela da saúde, em procedimento realizado por profissionais da saúde: utilizada quando, por exemplo, um cidadão se dirige a uma farmácia pública para obter remédios. O farmacêutico deverá ter acesso aos dados pessoais deste cidadão para verificar a medicação e realizar os controles necessários;

(vii) Para atender aos interesses legítimos do controlador ou de terceiro: pode ser utilizada para fundamentar atividades de tratamento de dados pessoais que tenham finalidades legítimas, consideradas a partir de situações concretas, como apoio e promoção de atividades da empresa, bem como para proteger os titulares de dados do exercício regular de seus direitos ou prestação de serviços que o beneficiem;

(viii) Para a proteção do crédito: esta base legal pode ser utilizada para serviços de proteção ao crédito.

Ressalta-se que, no caso de tratamento de dados pessoais sensíveis, não poderá ser utilizada a base legal do interesse legítimo. Além disso, segundo a LGPD, para o tratamento dos dados pessoais sensíveis, o consentimento deverá ser "específico e destacado, para finalidades específicas" (BRASIL, 2018), ou seja, o titular precisará ser informado exatamente para quais finalidades os seus dados pessoais serão tratados, devendo expressar o seu consentimento em uma cláusula em separado e em destaque do contrato original (por exemplo: assinando um anexo).

Há outra base legal para o tratamento de dados pessoais sensíveis, para a garantia de prevenção à fraude e da segurança do titular, em processos de identificação e autenticação de cadastro em sistemas eletrônicos: quando, por exemplo, é utilizada a biometria para acessar uma conta em um caixa eletrônico.


FBH
FEDERAÇÃO BRASILEIRA
DE HOSPITAIS

Seu hospital está preparado para a implantação e a aplicabilidade da Lei Geral de Proteção de Dados (LGPD)?

Conte com a FBH e suas Federadas para iniciarmos essa jornada juntos!

LGPD NA SAÚDE

A FBH, suas Federadas e a P&B iniciam uma parceria e criam um canal para ajudar os hospitais nesse desafio.

Quer saber mais?

Entre em contato com a FBH.

lgpd@fbh.com.br | fbh.com.br

FBH
FEDERAÇÃO BRASILEIRA DE HOSPITAIS

P&B COMPLIANCE | PAGLIA & BREUNIG

GUIA LGPD

PARA O SETOR HOSPITALAR

FBH
FEDERAÇÃO BRASILEIRA DE HOSPITAIS

P&B COMPLIANCE | PAGLIA & BREUNIG