MUST UNIVERSITY
FLORIDA - USA

Implementação da Lei Geral de Proteção de Dados (LGPD) em organizações de saúde

Implementação da Lei Geral de Proteção de Dados (LGPD) em organizações de saúde

Conteúdo organizado por **Millena Prata Jammal** em 2023 do livro **COMPLIANCE NA ÁREA DA SAÚDE**, publicado em 2020 pelos autores Andre Pontin, Angélica Carlini, Bruno Miragem, Christiane Bedini Santorsula, Clarice Seixas Duarte, Giovana Palmieri Buonicore, Giovani Agostini Saavedra, Hella Isis Gottschefsky, Heloisa de Carvalho Feitosa Valadares, Lara Rocha Garcia, Liliane Krauser Gomes, Roberta Scotto Menegazzo e pela editora Foco.

Objetivos de Aprendizagem

- Compreender sobre o processo de Implementação da Lei Geral de Proteção de Dados (LGPD) em organizações de saúde.

Introdução

Desde que a Lei Geral de Proteção de Dados entrou em vigor, a proteção de dados pessoais se tornou mais desafiadora para o setor de saúde. O que significa que as informações devem ser gerenciadas com uma abordagem mais abrangente.

As organizações de saúde devem ter procedimentos vigorados que possam ser acionados imediatamente para atender aos requisitos previstos na legislação. Isso se aplica ao setor público e privado: hospitais e clínicas, atendimento odontológico, farmácias, lares de idosos, laboratórios de diagnóstico, lojas que vendem produtos farmacêuticos e todas as outras empresas ou organizações que processam dados relativos à saúde.

Para evitar quaisquer violações, as organizações de saúde devem implementar os requisitos de conformidade com a LGPD, incluindo a gestão de contratos, bem como, políticas, procedimentos, documentação e registros de pacientes, profissionais de saúde e parceiros de negócio. Os registros da atividade de processamento de dados e os períodos de retenção e exclusão também devem estar adequados à lei de proteção de dados.

Princípios da LGPD

A LGPD possui 10 princípios, que têm como objetivos legitimar as bases legais para se realizar o tratamento de dados: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, responsabilização, prevenção, não discriminação.

A finalidade pressupõe que o dado será aplicado no tratamento informado ao titular, caso contrário, sua coleta se torna desnecessária.

Da mesma forma, o princípio da adequação preza pela compatibilidade do dado com o tratamento, bem como o princípio da necessidade, que exige que seja coletado o mínimo necessário. Todos os direitos do titular são pautados pelo princípio do livre acesso, a qualquer tempo pode solicitar informações sobre seus dados, assim como corrigi-los visto que a qualidade dos dados também é um princípio, assim como a transparência.

O emprego, ou até mesmo a ausência das melhores técnicas para a proteção está previsto no princípio da segurança e da responsabilização, em caso de incidentes. Para que isto não aconteça, o princípio da prevenção também está presente. Por fim, a não discriminação como princípio tem por objetivo impedir que sejam realizados tratamentos abusivos ou ilícitos.

Antes mesmo da LGPD, já havia entendimento internacional de que o paciente seria o detentor dos dados e que poderia ter acesso ao seu prontuário. Todavia, não previa a possibilidade de solicitar a exclusão ou o bloqueio de uso, por exemplo. Também o paciente, sem as previsões da LGPD, não saberia sobre qualquer compartilhamento, seja com farmácias, empregadores ou mesmo plano de saúde. Entender o caminho percorrido pelo dado que está sendo utilizado em qualquer tratamento foi permitido somente pela LGPD, como inovação legislativa.

Não somente as instituições de saúde lidam com dados de saúde, mas, basicamente, toda instituição o faz, especialmente de seus funcionários, se considerarmos os exames admissionais, demissionais, periódicos e eventuais atestados médicos, dados biométricos coletados nas catracas e sistemas eletrônicos de ponto. Configuram, todos estes itens em rol não extensivo, dados pessoais sensíveis previstos em lei e sujeitos à fiscalização da Autoridade Nacional de Proteção de Dados (ANPD), que está responsável por fiscalizar e aplicar sanções aos infratores, previstas no artigo 52, que podem ser aplicadas isoladas ou cumulativamente e sem ordem de preferência. Constam sanções de natureza leve, como advertência e publicização da infração para conhecimento do público em geral; intermediária, como bloqueio, eliminação ou suspensão do uso dos dados pessoais; e graves, como multa, suspensão do exercício da atividade de tratamento ou do banco de dados e até proibição total ou parcial das atividades relacionadas a tratamento de dados.

Qualquer informação compartilhada com convênios ou seguradoras precisam do consentimento expresso do titular, até porque isso pode ter impacto econômico e financeiro para todas as partes.

Muitos sistemas usados no setor de saúde agora são totalmente digitais. Com a ajuda da tecnologia baseada em nuvem, os sistemas que contêm dados do paciente são frequentemente compartilhados entre hospitais, farmácias e outras instituições, a fim de melhor atender os pacientes.

De acordo com a LGPD e considerando o fato de que os dados de saúde são constituídos por informações confidenciais de paciente, as instituições em saúde precisarão garantir que os princípios da Lei Geral de Proteção de Dados e Privacidade sejam devidamente cumpridos e demonstrar que seu processamento de dados atende aos requisitos específicos, que incluem a implementação de protocolos adequados que garantem a proteção dessas informações ao longo de todo o processo.

No entanto, este compartilhamento de dados é permitido para a realização de estudos em saúde pública (artigo 13), desde que tratados com segurança em ambiente controlado. Essa novidade legislativa tem sido bem aceita pelos pesquisadores, sem a necessidade do Termo de Consentimento Livre e Esclarecido (TCLE) para cada pesquisa que o pesquisador pretende fazer. Mesmo assim, restrições podem ser observadas. A finalidade deve ser exclusivamente para a pesquisa e o tratamento realizado somente no próprio órgão condutor do estudo, sem transmissão de dados a terceiros. Não obstante, sempre que possível, os dados deverão ser "anonimizados ou pseudoanonimizados" e, na divulgação dos resultados, não poderão ser revelados dados pessoais.

Qualquer empresa precisará passar por uma transformação cultural para estar em conformidade com a LGPD. Assimilar a soberania do titular, garantir que todos os seus direitos sejam possíveis de serem executados, fundamentar todos os tratamentos de dados existentes em bases legais de forma sólida e estruturada são ações complexas que não poderiam ser apenas parte de uma política ou discurso de liderança. Deve permear todos os funcionários, parceiros, terceiros e mesmo os clientes. A transparência e a ética essenciais ao *compliance* permeiam, também, os elementos de LGPD.

Dada a sensibilidade das informações pessoais relacionadas à saúde, elas só devem ser processadas por profissionais de saúde autorizados que estejam vinculados à obrigação de sigilo médico e de dados. Os indivíduos devem ser devidamente avaliados e lembrados de suas obrigações de confidencialidade. Além disso, é especialmente vital que as instituições de saúde realizem avaliações do impacto da proteção de dados e criem medidas de segurança específicas, como procedimentos de autenticação, uso de certificados e assinaturas digitais e controles de acesso aos dados pessoais de um paciente.

Da mesma forma, aplicar as melhores técnicas de engenharia de computação e desenvolvimento de *software*, em especial, normas de cibersegurança, também deve ser uma regra de *compliance* tecnológica.

Equipes formadas somente por profissionais das áreas jurídica e de *compliance* serão insuficientes para abarcar toda a complexidade de transformação de uma empresa. Transformar a mentalidade para que os dados estejam protegidos de forma contínua, durante o ciclo de vida das empresas, e impedir novas ações pode fazer com que a empresa atinja novo patamar de maturidade em ética, transparência e cuidado com o paciente. Fazer a gestão dos riscos e os treinamentos necessários são etapas fundamentais, mesmo porque os maiores riscos são de comportamento humano, mais do que tecnológicos.

Quando uma empresa não o faz, por vislumbrar os benefícios institucionais de respeitar o titular e atuar com transparência, acabará por fazer pela força da lei e das sanções.

Na prática, com a LGPD o paciente passa a ter os seguintes direitos previstos:

1. Ter direito à confirmação da existência de tratamento. Entende-se tratamento como toda a operação realizada com dados pessoais a exemplo de: coleta, produção, recepção, utilização, reprodução, transmissão, distribuição, processamento, arquivamento, modificação, comunicação, transferência, difusão, dentre outros;
2. Ter direito ao acesso e correção aos seus dados armazenados;
3. Anonimização (o dado anonimizado é relativo ao titular que não possa ser identificado);
4. Portabilidade;
5. Eliminação dos dados após o término do tratamento;
6. Informação a respeito do compartilhamento de dados;
7. Possibilidade de receber informação sobre não fornecer o consentimento e suas consequências;
8. Revogação do consentimento.

Se o controle de acesso não for adequado, pode facilmente levar a uma violação de dados e de acordo com a lei de proteção de dados a multas e sanções que podem comprometer a reputação e saúde financeira de qualquer instituição de saúde, independente do seu tamanho.

Redução do risco de violação de informações pessoais de pacientes

1- Garantir a conscientização

• **Entre os pacientes**: todos os titulares dos dados devem ser informados dos detalhes de terceiros com os quais suas informações serão compartilhadas, a fim de cumprir os requisitos de transparência estabelecidos pela LGPD. Além disso, o acordo de compartilhamento de dados deve definir claramente a finalidade, as bases legais e as informações a serem compartilhadas, juntamente com os detalhes necessários sobre o tratamento dos direitos dos titulares dos dados e os padrões de segurança que vão resguardar o compartilhamento desses dados.

• **Entre funcionários:** devem ser realizados treinamentos regulares de pessoal sobre a questão de proteção de dados, a fim de reduzir os riscos de erro humano e, portanto, de violação de dados internos. Conscientizar todos os funcionários sobre a importância da proteção de dados, as diretrizes que precisam ser implementadas e quais aspectos problemáticos típicos devem ser evitados pode ter um impacto positivo significativo nos esforços de conformidade de uma instituição.

2- Processe e compartilhe apenas os dados pessoais necessários para a finalidade do trabalho

É importante que os dados de saúde sejam processados minimamente e compartilhados apenas se necessário. A divulgação não autorizada pode ter um impacto sério na vida do paciente, portanto, deve-se garantir que o compartilhamento de dados seja feito com base em qualquer uma das bases legais de processamento, com acordos adequados em vigor para responsabilizar a parte responsável caso haja vazamento de dados. Para segurança e resguardo desses dados, eles só poderão ser compartilhados se:

• O titular dos dados deu consentimento explícito;

• Se o próprio paciente tornar os dados públicos;

• Quando se trata de uma situação de vida ou morte em que os pacientes não podem dar o seu consentimento e é do interesse vital do paciente;

- Para medicina preventiva ou ocupacional;
- Avaliação da sua capacidade de trabalho;
- Para diagnóstico médico;
- Para a prestação de cuidados de saúde ou assistência social ou tratamento ou a gestão de sistemas e serviços de saúde ou assistência social.

Deve-se salientar que as instituições de saúde devem manter a segurança dos dados durante todo o processo de compartilhamento.

3- Defina controles de acesso restritos

Dada a natureza compartilhada dos sistemas baseados em nuvem frequentemente usados no setor de saúde, é fundamental garantir que apenas aqueles necessários tenham acesso aos dados do paciente. A implementação de medidas como autenticação de dois fatores ou *login* único, assim como o uso de assinaturas e certificados digitais também podem ajudar a fornecer outras medidas para proteção de dados quando se trata de acessar arquivos de pacientes.

Saiba Mais

O que mudou para o setor de saúde após a LGPD?

Empresas que não se adequam à legislação podem ser punidas com multas milionárias, ficar com má reputação, ter problemas com parceiros e até mesmo ter dados excluídos.

Conceitos Fundamentais:

Anonimização - técnica de processamento de dados que remove ou modifica informações que possam identificar uma pessoa. Essa técnica resulta em dados anonimizados, que não podem ser associados a nenhum indivíduo específico.

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

Materiais Complementares:

1 - https://revista.unitins.br/index.php/humanidadeseinovacao/article/view/4183/2939. Acessado em 03 de janeiro de 2023.

2 - https://www.gov.br/ebserh/pt-br/hospitais-universitarios/regiao-nordeste/mejc-ufrn/comunicacao/noticias/mejc-realiza-acoes-visando-adequacao-a-lei-geral-de-protecao-de-dados. Acessado em 03 de janeiro de 2023.

Em Resumo

A forma como as informações são processadas e acessadas em organizações de saúde precisa ser ajustada, exigindo que as instituições de saúde fizessem da privacidade de dados sua principal prioridade. Os princípios da segurança da informação têm por objetivo proteger os dados contra acessos não autorizados e manter a disponibilidade para os donos dos dados, garantindo a primordialidade dos interesses dos pacientes e da própria instituição. A LGPD é benéfica para a sociedade, pois estabelece processos, papéis e dá transparência e respeito das relações entre instituição de saúde e paciente.

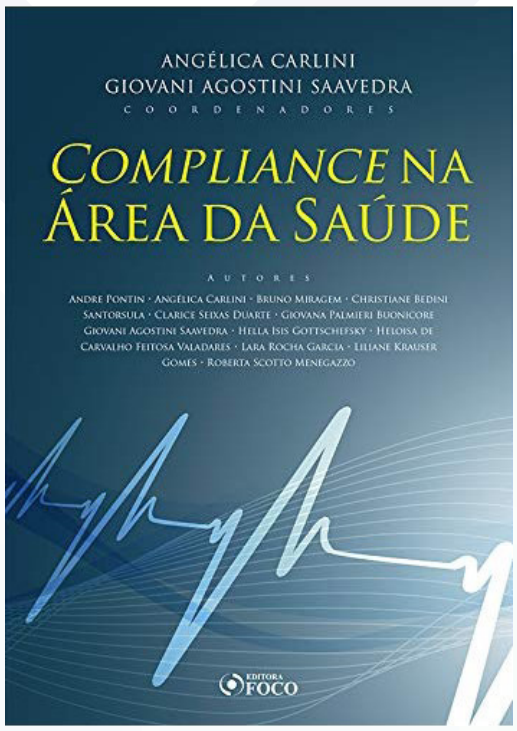
Na ponta da língua

Referências Bibliográficas

Frazão, A. N. A., Oliva, M. D., & Tepedino, G. (2019). *Compliance de dados pessoais*. In: Frazão, A. N. A., Oliva, M. D., & Tepedino, G. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 23-52. ISBN 978-85-5321-663-5.

Pontin, A. L., Angélica, C., Miragem, B., & Santorsula, C. B. (2020). *Compliance na área da saúde*. Indaiatuba, SP: Editora Foco.

Hawryliszyn, L. O., Coelho, N. G. S. C., & Barja, P. R. (2021). Lei Geral de Proteção de Dados (LGPD): o desafio de sua implantação para a saúde. *Revista Univap*, 27(54).



LIVRO DE REFERÊNCIA:

COMPLIANCE NA ÁREA DA SAÚDE

Andre Pontin, Angélica Carlini, Bruno Miragem, Christiane Bedini Santorsula, Clarice Seixas Duarte, Giovana Palmieri Buonicore, Giovani Agostini Saavedra, Hella Isis Gottschefsky, Heloisa de Carvalho Feitosa Valadares, Lara Rocha Garcia, Liliane Krauser Gomes, Roberta Scotto Menegazzo.

Editora Foco, 2020.

MUST UNIVERSITY
FLORIDA - USA

Imagens: Shutterstock