ALEXANDRE ATHENIENSE ADVOGADOS

www.atheniense.com

30 anos

A Lei Geral de Proteção de Dados

e seus efeitos para a prática médica e gestão de saúde

facebook.com/alexandreathenienseadvogados

ÍNDICE

Uma lei inovadora

Este e-book se destina a informar médicos, enfermeiros e todos que trabalham na gestão dos serviços de saúde sobre os impactos da recentemente aprovada Lei Geral de Proteção de Dados Pessoais. Essa lei, seguindo a tendência de mais de 100 países no mundo, se destina a regulamentar a coleta, a produção, a recepção, a classificação, a utilização, o acesso, a reprodução, a distribuição, o processamento, o arquivamento, o armazenamento, a eliminação, a avaliação ou o controle de informações pessoais recolhidas com intenções econômicas, para proteger os cidadãos contra o mau uso dessas informações ou contra a negligência quanto à segurança desses dados.

No entanto, muitas das obrigações introduzidas pela nova lei correspondem a rotinas operacionais que não fazem parte da rotina procedimental de um médico ou rede de saúde. São totalmente inovadoras e é necessário que o mercado de todos os setores se adapte às mudanças, que passam a valer oficialmente no início de 2020. Para os médicos e demais profissionais da saúde, que lidam com dados pessoais de terceiros, é preciso redobrar a atenção para garantir a segurança dos dados e o tratamento em conformidade com a nova lei. O objetivo deste e-book é explicar de forma objetiva e clara algumas das principais questões relacionadas ao assunto, como uma orientação inicial aos médicos e outros profissionais da saúde para o processo de adaptação à nova lei. Nas páginas a seguir estão respostas a 13 perguntas fundamentais para compreender o impacto da Lei Geral de Proteção de Dados Pessoais na prática médica e gestão de saúde.

Alexandre Atheniense, especialista em direito digital e sócio-fundador do Alexandre Atheniense Advogados

Colaborou na elaboração deste e-book a acadêmica ***Luísa Côrtes Grego***

13 questões fundamentais sobre a Lei Geral de Proteção de Dados para profissionais e gestores de saúde

A seguir apresentamos perguntas e respostas como uma orientação inicial ao processo de adaptação à nova Lei Geral de Proteção de Dados Pessoais, que passará a vigorar em 16 de fevereiro de 2020.

1) Algum médico já foi punido por violar a proteção de dados de pacientes no Brasil?

O Brasil já teve vários casos de médicos violando o sigilo de dados de seus pacientes. Um mais recente e destacado foi o caso de uma radiologista, que expôs em um grupo de WhatsApp informações não autorizadas sobre o estado de saúde da falecida Marisa Letícia Lula da Silva, ex-primeira dama. A médica, que à época trabalhava no Hospital Sírio-Libanês, onde a paciente estava internada, foi demitida e o Hospital, em nota, disse repudiar sua conduta e ter "uma política rígida relacionada à privacidade de pacientes".

2) Essa punição foi com base na nova lei?

Esse e outros casos não foram julgados pela Lei Geral de Proteção de Dados, pois ela só começa a valer em fevereiro de 2020, para dar tempo de adaptação à sociedade. Até lá, aplicam-se as regulações anteriores, como o Código de Defesa do Consumidor e as leis que tratam da fiscalização de atividades farmacêuticas, regulações da ANVISA, do CFM e dos CRM, relativos ao sigilo profissional e publicidade médica, que já definem obrigações para os médicos em relação à proteção das informações e da privacidade do paciente. A LGDP reúne essas obrigações e as amplia.

3) O que a nova lei determina no que diz respeito à saúde?

A Lei Geral de Proteção de Dados Pessoais define a natureza das informações coletadas nas atividades da saúde como dados pessoais sensíveis. Isso é, esse tipo de dado merece a mais rígida proteção, por se relacionarem à esfera íntima da pessoa, trazendo maior risco e potencialização de danos em casos de exposição ou vazamento. No grupo de informações sobre saúde estão incluídas:

- As receitas médicas
- Os diagnósticos
- Os exames
- Os dados dos planos de saúde
- Qualquer dado referente à identidade da pessoa - como RG, CPF, nome, dados de contato, características físicas, etc..

4) Nenhum dado de saúde pode ser compartilhado, então?

Uma das poucas permissões concedidas para tratamento de dados sensíveis se refere à tutela da saúde. Os profissionais que utilizam esses dados para fins econômicos são obrigados a obter o "consentimento expresso e informado" do paciente (titular), e esse uso só pode acontecer de acordo com a finalidade da coleta que é lhe dada ciência no momento do consentimento. Sempre que possível, os dados pessoais devem ser "anonimizados" ou "pseudonimizados" para compartilhamento. Isso significa que, sempre que for possível, o profissional deve tratá-los de forma em que o titular não seja identificado ou identificável – dissociando a identidade do paciente das informações a serem usadas, evitando exposição desnecessária ou desmedida de sua privacidade mesmo quando o dado é acessado e compartilhado.

Portanto, a regra geral é o consentimento do titular, mas existem exceções. Uma delas, por exemplo, é a possibilidade de risco de morte do paciente ou sua integridade física.

Por outro lado, aqueles que descumprirem a lei estão sujeitos a advertências, multas que vão de 2% do faturamento anual da empresa ou até R$ 50 milhões por infração, além de multas diárias variáveis.

5) Que tipos de cuidados os médicos devem passar a tomar a partir de agora?

O que muda é a forma de lidar com os dados dos pacientes, que, para ser compreendida, passa por algumas perguntas específicas respondidas a seguir:

6) Qual é a forma correta de obter consentimento para a coleta de dados? Existe algum cuidado especial a ser tomado na proteção de dados de menores de 18 anos?

A lei define como consentimento a permissão expressa do titular do dado que o identifica para a coleta, tratamento e eventual compartilhamento das informações obtidas. Como é sabido, a Ética Médica exige dos profissionais o esclarecimento ao paciente antes do procedimento médico e o seu consentimento expresso, salvo em iminente perigo de vida. Além disso, obriga o médico a informá-lo sobre "o diagnóstico, o prognóstico, os riscos e objetivos do tratamento". O descumprimento dessas obrigações é considerado omissão do dever de informação e é visto como negligência.

No mesmo sentido, a Lei Geral de Proteção de Dados conceitua "consentimento

informado" como atividades que não se resumem somente a essas obrigações de informação ao paciente quanto ao seu tratamento médico, expandindo para a necessidade de assegurar o consentimento informado para o tratamento e coleta de dados pessoais. Para os menores de idade, todas as obrigações de informação devem ser prestadas aos seus representantes legais (pai, mãe ou tutor), que são os responsáveis pelo consentimento expresso.

Percebe-se que vários procedimentos operacionais deverão ser revistos para estarem em conformidade legal. Os maiores destaque são o consentimento expresso, a obrigação de informar a finalidade para a coleta de dados e a possibilidade do paciente revogar seu consentimento, caso que gera a obrigação de remoção de dados por parte do profissional.

7) E se eu precisar compartilhar as informações pessoais de pacientes com outros médicos ou clínicas. Quais cuidados devo estar atento?

O compartilhamento de dados pessoais entre médicos sobre pacientes é uma das poucas exceções às restrições para tratamento de dados sensíveis. Isto pode acontecer, mas deve sempre ocorrer da forma mais segura possível - ou seja, usando mecanismos de proteção de dados e privacidade para que o compartilhamento não desejado para pessoas que não tenham relacionamento direto com a prática profissional médica.

Para garantir a privacidade dos pacientes, um mecanismo que pode ser usado é a omissão da identidade destes ao compartilhar os dados (anonimização) ou a substituição da sua identidade por outra fictícia (pseudonimização). É importante ter cuidado para que, dentro do ambiente de trabalho, somente tenham acesso aos dados pessoais de pacientes aqueles que de fato precisam ter,

respeitando a finalidade da coleta e evitando casos de negligência ou vazamento proposital que possam vir a ocorrer.

Segurança nos dados é garantir a sua boa administração e governança, então é preciso mapear os riscos, enxergar as lacunas atuais, planejar, modificar processos internos para estar em conformidade com a lei e verificar sempre os procedimentos executados em relação aos dados pessoais de terceiros que estão sendo tratados. Também é necessário ter em mente que, a após a sanção da Lei de Proteção de Dados Pessoais, exercer a governança digital e investir em capacitação e segurança da informação capaz garantir mais recursos do sigilo, não deve ser visto como um custo, mas sim um diferencial de mercado.

8) E se os dados forem vazados ? Eu posso ser considerado responsável por este incidente de segurança ? Quais medidas devo tomar para o enfrentamento para reduzir o risco?

Sim, o responsável pela clínica é um dos responsáveis no caso de vazamento de informações. Na legislação brasileira, todos que exercem o tratamento dos dados pessoais de terceiros para fins econômicos são considerados como controladores. Daí a responsabilidade legal e o risco de penalidades poderá inclusive se os atos praticados forem praticados forem praticados por agentes externos terceirizados para tratar os dados pessoais. Portanto, a partir de agora o vazamento de dados implicará na responsabilização do profissional de saúde ou sua organização pelo ato e quanto aos danos causados, devido às vulnerabilidades da segurança da informação. No mundo cada vez mais digital, devemos adotar estratégias de proteção e segurança de dados, para evitar o risco de perdas financeiras assim como protegemos o dinheiro.

É importante perceber que a cada dia, os dados, sobretudo aqueles sensíveis que revelam a esfera íntima das pessoas, adquirem valor próprio, se tornam um ativo cada vez mais valioso, e por estes motivos merecem maior governança.
É necessário refletir sobre as medidas operacionais e jurídicas a serem tomadas que conjuguem sistemas de segurança mais apropriados, adotar medidas jurídicas procedimentais para reduzir riscos, criar novos processos internos e capacitar a equipe, para mitigar os riscos de vazamento e outros incidentes relativos aos dados de terceiros. Além disso, será necessário colocar em prática um efetivo sistema de contingenciamento com apoio jurídico especializado para agir no tempo mais breve possível após o incidente. O aumento do dano está ligado diretamente ao tempo de resposta para enfrentamento em conformidade legal.

Pela nossa experiência profissional, quando ocorre um vazamento de dados numa empresa, normalmente demora em média 90 (noventa) dias para identificar o incidente. Ou seja, o agente já vem operando sem ser notado há um período muito superior do que se imagina. Com a adoção de um plano de contingenciamento sistêmico e jurídico será possível abreviar estas medidas de forma a reduzir os riscos. Caso não haja um plano de contingenciamento, o enfrentamento será tardio e desordenado e o prejuízo pode ser imensurável - já que a organização é responsável e deve indenizar qualquer dano ou prejuízo decorrente do vazamento de informações do paciente/consumidor.

A necessidade de indenizar, nesse caso, independe da culpa da instituição, por ela exercer uma atividade “de risco” e, quando o risco gera dano, ela precisa arcar com ele. Para que o plano de contingenciamento seja efetivo é fundamental que ocorra a capacitação dos colaboradores para que cada um saiba em que momento correto e o prazo limite para cumprir suas obrigações neste processo.

O que a minha equipe precisa fazer?

- Manter todos os sistemas de todas as máquinas atualizado
- Não compartilhar senhas
- Sempre consultar os responsáveis pelo TI quando não souber realizar alguma função
- Só instalar programas e aplicativos nas máquinas quando expressamente autorizados
- Nunca baixar arquivos sem saber o que são
- Nunca clicar em links sem saber o que são
- Orientar os pacientes sobre seus direitos de forma clara e coerente e revelar qual será a finalidade do tratamento de dados em conformidade com a legislação atual
- Quando ocorrer um incidente, saber como preservar as provas em conformidade legal
- Buscar orientação jurídica especializada o mais breve possível para definir quais medidas extrajudiciais e judiciais serão tomadas de modo a abreviar o enfrentamento e reduzir o risco.

O que eu preciso fazer?

- Mudar todas as senhas periodicamente
- Manter todo o sistema atualizado
- Pesquisar histórico de falhas de segurança de todos os programas que cogitar usar
- Fazer um sistema de segurança de acordo com a expectativa legal
- Fazer um plano de contingenciamento técnico e jurídico
- Garantir que os processos operacionais relativo aos dados pessoais de terceiros estejam em conformidade legal
- Manter registro de todas as medidas que estão sendo tomadas em relação à segurança, como exige a Lei
- Orientar os pacientes sobre seus direitos de forma clara e coerente e revelar qual será a finalidade do tratamento de dados em conformidade com a legislação atual
- Quando ocorrer um incidente, saber como preservar as provas em conformidade legal
- Buscar orientação jurídica especializada o mais breve possível para definir quais medidas extrajudiciais e judiciais serão tomadas de modo a abreviar o enfrentamento e reduzir o risco.

9) São os funcionários da clínica que coletam os dados pessoais de terceiros. Eu ainda sou o responsável e posso ser punido?

Sim. A Lei Geral de Proteção de Dados atinge qualquer um que colete dados, seja na internet ou não. Quando a sua secretária coleta dados para serem usados durante a sua prática médica, em espaço profissional que você controla, ela está agindo em seu nome, como sua subordinada, e a responsabilidade por seguir a lei é de todos os envolvidos - ela, você como médico, a clínica ou o hospital em questão. Isso significa que, se a sua clínica coleta dados ou a sua secretária coleta em seu nome, você é o responsável pela preservação, tratamento e armazenamento correto desses dados e pode ser obrigado a indenizar em caso de vazamento que gere prejuízo ao titular do dado. Caso ela aja sozinha, em nome próprio, gerando o dano, a responsabilidade por proteger os dados será ainda assim sua e você pode, mesmo assim, ser responsabilizado. Caso você armazene os dados incorretamente e ocorra vazamento ou outro problema, a responsabilidade por armazenamento será diretamente sua, da clínica ou do hospital.

10) Uso um sistema de agenda exercida por um prestador de serviço terceirizado. Eu serei o responsável e posso ser punido caso este cometa algum incidente de segurança de dados?

Sim. O médico que requisita as informações de seus pacientes é responsável pelo tratamento de dados, mesmo quando esta atividade seja executado por prestador de serviço. No caso de vazamento que gere danos a terceiros, a indenização pode ser fixada tanto da empresa que fornece a agenda quanto do controlador dos dados, ou seja, do médico que os requisitou. Nesse caso, se a culpa for da empresa, o médico pode, depois de paga a indenização, exigir que

a empresa prestadora de serviços lhe compense, mas isso requer outro processo judicial e pode demorar. De qualquer forma, é altamente recomendável que os contratos de prestação de serviços sejam revisados em conformidade com a Lei de Proteção de Dados.

11) Como eu devo mudar a minha forma de lidar com os dados pessoais dos pacientes?

Ao falarmos de dados, o maior risco em termos financeiros será quando ocorrer vazamento - ou seja, na possibilidade de exposição dos dados íntimos de saúde de pacientes para terceiros que não têm autorização para ter acesso a eles. Para evitar isso, cinco medidas são essenciais para garantir a adequação à lei:

- **Sistema de segurança** que proteja esses dados compatível com os riscos específicos da sua forma de armazená-lo, construído de acordo com as necessidades do seu negócio.

- **Plano de contingenciamento sistêmico e jurídico** capaz de abreviar o tempo de enfrentamento e reduzir os danos de um eventual vazamento.

- **Registro de todas as atividades** tomadas para tratamento dos dados e as medidas de segurança aplicadas, já que este procedimento poderá ser decisivo numa decisão judicial.

- Caso ocorra o vazamento ou outro incidente com os dados pessoais de terceiros gerando para o seu paciente ou pessoa a ele relacionada, deverá ser executado na maior brevidade possível um **processo investigatório interno**, com o objetivo de descobrir se houve ou não negligência no tratamento dos dados.

- **Dar ampla ciência** por meio de uma **comunicação pública ou direcionada** para as vítimas, da extensão do dano causado e quais as medidas jurídicas ou operacionais que devem ser adotadas para reduzir o risco.

Além disso, o armazenamento de dados deve obedecer as exigências determinadas pela Lei Geral de Proteção de Dados e de normas regulatórias. O que a legislação brasileira determina é que todo o sistema de armazenamento, tratamento e segurança dos dados precisa estar de acordo com a tecnologia compatível para executar esses serviços com eficiência e segurança - ou seja, não é preciso ter o melhor sistema de segurança disponível no mercado para estar em conformidade legal, mas é preciso adotar um modelo compatível com os padrões utilizados mundialmente para esta finalidade.

Medidas para estar em conformidade

- Revisar o termo de consentimento do paciente, para que ele se adeque à noção de "consentimento expresso e informado" da nova Lei de Proteção de Dados, revelando a finalidade da coleta de dados, os limites do tratamento e a possibilidade da revogação do consentimento no futuro.
- Adotar medidas de proteção dos dados: contar com a consultoria de especialistas para montar um plano de contingenciamento de segurança digital e de medidas legais para abreviar o tempo de resposta reduzindo o alcance dos riscos e prejuízos financeiros.
- Criar um canal de comunicação que permita ao paciente a revogação do consentimento do tratamento de seus dados pessoais
- Tornar anônimos ou pseudônimos os dados de saúde compartilhados com terceiros
- Capacitar os colaboradores sobre segurança da informação e proteção de dados exemplificando os riscos legais e as medidas procedimentais que serão implantadas
- Manter atualizado quanto às melhores práticas operacionais para o tratamento dos dados pessoais de terceiros

12) O que acontece se os dados dos meus pacientes vazarem?

Se os dados dos pacientes vazarem, o médico será obrigado a informá-los publicamente sobre a ocorrência deste incidente e qual a extensão da exposição das vítimas. Esta medida deverá ocorrer na maior brevidade possível a partir do momento em que se toma conhecimento do fato, além de tomar medidas urgentes operacionais e jurídicas para o enfrentamento. A partir deste momento, os pacientes podem ou não sofrer danos decorrentes deste incidente, sendo possível o ajuizamento de medida judicial para reparação de danos.

Os responsáveis pelo tratamento dos dados pessoais de terceiros, ou seja, a clínica ou hospital, os terceirizados responsáveis por prestar serviços, ou qualquer outra entidade, instituição ou pessoa que têm responsabilidade sobre a proteção dos dados poderão responder solidariamente numa medida judicial que busca a reparação dos danos e indenização das vítimas. Por causa desse risco, é importante que a ciência pública sobre o vazamento, seja estruturada de forma a atender a obrigação legal, sem expor em demasia a clínica ou hospital, pois tal ato irá colocar em risco sua reputação e o modelo de negócio, ou mesmo sua eventual defesa processual. Por tais motivos é altamente recomendável contar com profissionais especializados.

13) Como eu crio um plano de segurança e um plano de contingenciamento?

Estes planos demandam adequação à conformidade legal. É recomendável que a equipe destacada para executar estas atividades contém um profissional especializado em Direito Digital, além de um profissional da área de TI, um responsável pela área de Governança, um representante do setor de Recursos

Humanos e de Comunicação, além da coordenação de um responsável que tenha poderes decisórios. Em relação aos procedimentos técnicos, eles devem ser executados por meio de sistemas especialistas de processamento e armazenamento de informações que possam geram robusta trilha de registros eletrônicos para facilitar o processo investigatório de identificação de autoria do agente que cometeu o ilícito e outros responsáveis.

Quanto à lacuna de capacitação dos colaboradores, é necessário investir em treinamentos e na formalização da ciências desta bem como da Política de Segurança da Informação, que é um ato normativo necessário de uso interno, que defina os limites de uso da infraestrutura de tecnologia da informação, os procedimentos a serem adotados pelos colaboradores e prestadores de serviço as permissões de acesso, locais ou remotos e os dados tratados pela organização.

O plano de contingenciamento é um plano que envolve respostas jurídicas e tecnológicas para possibilitar a apuração e o enfrentamento com a maior brevidade possível após o incidente, de modo a tomar medidas corretivas em conformidade legal para reduzir os riscos e prejuízos financeiros envolvidos.

O zelo às regras de proteção de dados e privacidade, embora envolva uma série de medidas operacionais complexas, e até então inimagináveis, deve ser encarado pelos médicos e organizações de saúde não apenas como custo, mas sim como um diferencial para competitividade no mercado, de modo a potencializar e adequar uma reputação de credibilidade perante seus colaboradores e clientes. Tais medidas se revelam como novos hábitos para combater aos novos riscos da economia digital globalizada lastreada em dados que se tornaram ativos importantes e regulados pela legislação brasileira e atos regulatórios.

ALEXANDRE ATHENIENSE ADVOGADOS | DIREITO DIGITAL

www.atheniense.com

FALE COM A GENTE

www.atheniense.com
facebook.com/alexandreatheniense advogados
contato@alexandreatheniense.com.br
São Paulo • Belo Horizonte • Brasília

Alexandre Atheniense é advogado formado pela Universidade Federal de Minas Gerais (UFMG), especializado em Internet Law na Berkman Center – Harvard Law School e sócio-fundador do Alexandre Atheniense Advogados.

Com experiência profissional de 30 anos é um dos precursores do Direito Digital no Brasil. Possui vasta experiência acadêmica e institucional, tendo exercido por oito anos (2002-2010) a presidência da Comissão de Tecnologia da Informação da OAB Federal, representando a entidade na discussão de projetos de lei no Congresso Nacional sobre os temas relacionados a Tecnologia da Informação, Coordenador da Comissão de Direito Digital do CESA - Centro de Estudos das Sociedades de Advogados, Árbitro em questões relacionadas à Propriedade Intelectual e Tecnologia da Informação na Camarb, CAMINAS e ABPI e autor diversas obras sobre Direito Digital no Brasil e no exterior.

ALEXANDRE ATHENIENSE
ADVOGADOS

www.atheniense.com

30 anos

www.atheniense.com

facebook.com/alexandreatheniensead vogados

contato@alexandreatheniense.com.br