SBGM
Sociedade Brasileira de Genética Médica e Genômica

A LGPD na prática da Telemedicina

Dra. Sandra Franco
Contribuição: Dr. Raphael Moraes

GRUPO DE TRABALHO DE TELEMEDICINA SBGM I GESTÃO 2021/2023
São Paulo, agosto de 2023

SUMÁRIO

Como estar em conformidade com a LGPD em consultórios e clínicas?

A sociedade passa por uma transformação, em decorrência do impacto da tecnologia na gerência das nossas vidas, bem como pela presença de um inimigo invisível, a pandemia, que modificou a forma de nos relacionarmos. A sociedade como conhecíamos foi modificada. E nessa modificação, nossa relação com o ambiente virtual deixou de ser exceção para se tornar regra.

Nessa condição, nossas informações pessoais passaram a se caracterizar como a nova moeda de troca da sociedade. Sim, os dados. Sobre isso, o filósofo polonês Bauman pontuou na sua teoria de relações líquidas, no sentido de que, quando desejamos o objeto, nos tornamos objeto de desejo.

Praticar a Telemedicina com segurança dos dados e primando pela confidencialidade dos dados do paciente é um desafio. Não basta apenas se preocupar com a escolha de um software seguro; faz-se necessário mudar o comportamento dentro da clínica ou do consultório. Repensar na prática o quanto a busca por facilidade compromete a exposição dos dados do paciente, por exemplo, a colaboradores.

Serão expostos aqui um pouco da teoria para se entender a importância da proteção de dados no contexto atual, a lei específica hoje vigente (a LGPD) e algumas orientações sobre como se adequar a essa lei. Evidente que não se pode esquecer do Marco Civil da internet, Constituição Federal, Código de Defesa do Consumidor, Normativas da ANS (Agência Nacional de Saúde Suplementar), Normativas trazidas pela Política Nacional de Segurança da Informação e , claro, o Código de Ética Médica, além das resoluções específicas do CFM (Conselho Federal de Medicina).

Parece muita coisa? De fato é! Mas, traremos aqui as principais diretrizes. Vamos lá!

1. Um pouco sobre o direito à privacidade e ao sigilo

A preocupação com a privacidade, o sigilo e a intimidade do ser humano já existe há muito tempo. Trata-se de direitos humanos, positivados em textos nacionais e internacionais, em especial na Declaração Universal dos Direitos Humanos, em seu art. XII: "Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação."

Na Medicina o conceito de privacidade é apontado no juramento de Hipócrates, no qual ele aponta a confidencialidade das informações do paciente. Agora, mais do que nunca, a confidencialidade é transmutada em privacidade, pontuada por uma legislação específica e que vem carregada por uma revolução nas formas e conteúdos através da digitalização da profissão.

O sigilo do médico quanto às informações do paciente é fundamento ético inalienável. Há outros dispositivos em nosso ordenamento com o propósito de salvaguardar esse mandamento: o Código Penal caracteriza como ilícito penal a revelação de segredo a que se teve ciência no exercício da profissão, o Código de Processo Civil e o Código de Processo Penal dispõem que ninguém será obrigado a depor sobre fato a cujo respeito, por profissão, deva guardar segredo.

No processo de positivação no ordenamento jurídico brasileiro, tem-se, na Constituição Federal brasileira de 1988, esse mesmo direito contido no art. 5°, inciso X: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

Em fevereiro de 2022, deu-se mais um passo importante para a valorização do tema da proteção de dados, através da publicação da EMENDA CONSTITUCIONAL Nº 115, a qual inclui a proteção de dados pessoais entre os direitos e garantias fundamentais e fixa competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

No âmbito médico, o Código de Ética Médica (CEM) apresenta, de forma mandatória, a observância ao sigilo, em vários artigos: "Vedado revelar...", " fazer referência a casos clínicos identificáveis", "revelar informações confidenciais, inclusive de trabalhadores por exigência do empregador", "prestar informação à empresa seguradora sobre as circunstâncias da morte do paciente, além das contidas no atestado de óbito", "deixar de orientar seus auxiliares a respeito do sigilo", "deixar de guardar na cobrança de honorários o sigilo profissional", "revelar sigilo profissional relacionado a paciente menor de idade", e mais uma gama de dispositivos versando sobre o tema.

Também se encontram contemplados o sigilo e a confidencialidade na Lei de Acesso à Informação (Lei nº 12.527/2011), no Marco Civil da Internet (Lei nº 12.965/14) e na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.708/2018), a qual será tratada mais adiante.
Em suma, o tema da privacidade, do sigilo profissional, mais do que nunca se encontra balizado por diversas normas e especificamente pela Lei Geral de Proteção de Dados.

A privacidade e a segurança de dados são dois temas atuais e que precisam ser discutidos para que se possam criar normas que permitam o aproveitamento dos benefícios que a tecnologia oferece à sociedade, observando-se que a informação de cada paciente é confidencial e apenas diz respeito a ele próprio e a seu médico ou pessoas por ele autorizadas.

Aqui se destaca outro princípio importante na Medicina e no próprio Código de Defesa do Consumidor: a autonomia do paciente. Inconteste que o uso da tecnologia se faz essencial para ampliar o acesso à saúde. De outro lado, a incorporação precisa ser feita com segurança para que não se atropelem os direitos dos pacientes à privacidade, sigilo, confidencialidade, intimidade, imagem e honra.

O Registro Eletrônico de informações do paciente, por exemplo, é hoje uma ferramenta muito valiosa. A Resolução CFM nº 1821/2007 apresenta as normas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. O pilar dessa Resolução está em apresentar requisitos técnicos que permitam garantir o direito ao sigilo e à confidencialidade das informações do paciente. Foi aprovado o Manual de Certificação para Sistemas de Registro Eletrônico em saúde[1], que traz normas para a eliminação do papel, com critérios determinando o NGS1 (Nível de Garantia de Segurança 1) para os sistemas eletrônicos, não sendo possível, porém, eliminar o papel pela ausência da assinatura digital, contemplada apenas para os sistemas com NGS2 (Nível de Garantia de Segurança 2).

Recentemente, duas importantes resoluções foram publicadas pelo Conselho Federal de Medicina. Uma está relacionada a regras específicas para emissão de documentos médicos eletrônicos, a Resolução CFM Nº 2.299, de 30 de Setembro de 2021, que normatiza a emissão de documentos médicos eletrônicos.[2]

Destaque para a exigência contida no § 2º do Art. 3º, no sentido de que deve ser assegurado cumprimento integral à Lei Geral de Proteção de Dados (LGPD). Tarefa nada fácil.
Outro importante texto, a Resolução CFM nº 2.314, de 20 de abril de 2022[3], foi publicado com o objetivo de regulamentar a telemedicina. Entre outras importantes diretrizes está descrito o dever do médico de proteger os dados pessoais e clínicos do teleatendimento médico, segundo as definições da LGPD e outros dispositivos legais.
É preconizado por profissionais de segurança da informação que profissionais e instituições de saúde se utilizem de documentos eletrônicos, protegidos por criptografia e armazenados em nuvem por serem mais seguros do que o papel. De outro lado, por sempre ter o risco

1. www.sbis.org.br

2. www.in.gov.br

3. www.in.gov.br

de vazamento de dados, será necessária a observância de diretrizes normativas e legais para o tratamento desses dados.[4]
Conforme o princípio da segurança, todas as informações precisarão estar em ambientes controlados e comprovadamente seguros. Além disso, também é de suma importância implantar soluções de segurança (segundo as possibilidades de cada organização). Para tanto as instituições deverão adotar redes criptografadas, softwares de monitoramento, mas especialmente preparar as pessoas que terão acesso aos dados, já que o ser humano é o elo mais fraco na cadeia da segurança.

Para entender a privacidade na genética, é necessário primeiro mergulhar no complexo conceito de privacidade. Privacidade é um estado de acesso limitado a um indivíduo ou informações sobre um indivíduo. O direito à privacidade refere-se aos princípios éticos e legais que reconhecem a importância do acesso limitado a um indivíduo ou a informações sobre um indivíduo. Anita Allen propôs quatro categorias de privacidade aplicáveis ao que ela chama de "um conceito ambíguo de privacidade genética".

Quando usado para rotular questões que surgem na bioética contemporânea e nas políticas públicas, 'privacidade' geralmente se refere a uma das quatro categorias de preocupação. São elas: (1) privacidade informacional: preocupações sobre o acesso a informações pessoais; (2) preocupações de privacidade física: sobre acesso a pessoas e espaços pessoais; (3) preocupações de privacidade decisórias: sobre questões governamentais e outras interferências de terceiros em escolhas pessoais; e (4) preocupações de privacidade proprietária: sobre a apropriação e propriedade de interesses na personalidade humana[5].

Do enorme conjunto de dados que é o genoma de todo ser humano a pedigrees familiares e resultados de testes genéticos, a genética está intimamente associada à informação. Genômica e abordagens analíticas relacionadas - como proteômica, metabolômica, transcriptômica e epigenômica – aumentam muito a quantidade de informações potenciais associadas a genes sobre indivíduos.
A informação genética é sensível porque tem implicações para a saúde atual e futura dos indivíduos e suas famílias. A informação também pode ter grandes consequências sociais e econômicas, Obviamente, nos termos da LGPD, o dado genético é classificado como um dado sensível, artigo 5°, inciso II da LGPD.

4. Para entendimento dos termos utilizados na LGPD, esclarece-se que tratamento dos dados é qualquer ação ou operação com dados pessoais.

5. Anita L. Allen, Genetic Privacy: Emerging Concepts and Values, in GENETIC SECRETS: PROTECTING PRIVACY AND CONFIDENTIALITY IN THE GENETIC ERA 31, 33 (Mark A. Rothstein ed., 1997).

2. A Lei Geral de Proteção de Dados (LGPD)

Influenciado pelo GDPR (General Data Protection Regulation) europeu, o Brasil publicou a nova Lei Geral de Proteção de Dados (Lei n° 13.709/2018), que representa uma inovação na regulamentação do tema no país, na esteira do Marco Civil da Internet.

Conforme disposto em seu art. 1°, a LGPD dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica, de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Importante contribuição da LGPD é a clara enunciação do conceito de dados, contemplada em seu art. 5°. Como se encontra ali disposto, tem-se:

I- Dado pessoal – informação relacionada a pessoa natural identificada ou identificável;

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

III- Dado pessoal sensível – 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; e dado genético ou biométrico, quando vinculado a uma pessoa natural.

2.1. Agentes de Tratamento na lei: o Controlador e o Operador

Consoante disposto na LGPD, os agentes de tratamento de dados são aqueles que manipulam os dados dos titulares.
Controlador: pessoa natural ou jurídica a quem compete as decisões referentes ao tratamento de dados pessoais; II) Operador: pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.

No consultório, podemos classificar o médico como sendo o controlador dos dados. A empresa de software do prontuário eletrônico, por exemplo, é o Operador.

As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais. Além disso, a guarda e a disponibilização de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. A lei ressalta ainda a necessidade de eliminação definitiva destes dados ao requerimento do titular ou ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei. Na área de saúde, temos uma lei específica, do prontuário eletrônico[7], que determina a guarda por no mínimo 20 anos, o que, portanto, impede que haja a eliminação dos dados a pedido do titular.

No art. 17 está previsto que toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade; assim, a LGPD determina quais são as condições de proteção desses direitos fundamentais. A aludida Lei menciona as sanções cabíveis, podendo ser desde advertências, a multas de até 2% (dois por cento) do faturamento do grupo por infração por dia, ou até a proibição de exercício das atividades (não isentando empresas estrangeiras de responderem solidariamente às suas filiais).

Na relação médico e paciente, é importante que sejam preservados os direitos dos pacientes enquanto titulares. Mas, existem também outros "titulares", ou seja, outras pessoas físicas que também terão seus dados pessoais coletados e utilizados, como os próprios funcionários das clínicas e consultórios, além de representantes dos fornecedores de materiais. Estes também precisarão ter seus direitos protegidos e,

7. www.planalto.gov.br

para tanto, recomenda-se a criação de um programa de governança em privacidade, conforme determinado pela LGPD, que deverá ser desenvolvido segundo as características de cada negócio e o volume de dados tratados. A Lei Geral de Proteção de Dados coloca o titular do dado no controle de suas informações pessoais. Portanto, a partir da vigência da lei, o setor de saúde deverá ser capaz de garantir os direitos dos titulares dos dados, previstos em seu art. 18 (objeto de um capítulo à parte mais à frente).

A adequação à norma engloba todos os dados pessoais a que um profissional ou empresa de saúde tenha acesso, como os dados dos funcionários, fornecedores e dos próprios médicos, por exemplo.
É importante destacar que a área de saúde já é bastante regulada, de forma que os direitos dos pacientes precisam ser interpretados e compatibilizados de acordo com as normas já existentes do setor, como, por exemplo, o direito de acesso ao prontuário médico (ver Código de Ética Médica[8] e Lei do Prontuário).

Além disso, um dos maiores desafios do projeto de adequação à LGPD é a instrumentalização dos direitos dos titulares. É importante planejar o procedimento formal através do qual os titulares de dados poderão solicitar o exercício dos seus direitos e disponibilizar um canal de comunicação, amplamente divulgado, para assegurá-los de que as solicitações serão analisadas e atendidas sem demora injustificada, dentro do prazo estabelecido pela LGPD ou pela Autoridade Nacional de Proteção de Dados. Os consultórios e clínicas médicas não podem esquecer também de confirmar a identidade do titular do dado antes de disponibilizar as informações requeridas para evitar o compartilhamento indevido de dados com terceiros e a ocorrência de incidente de segurança da informação, popularmente conhecido como vazamento de dados. Ao verificar a identidade do titular do dado, é importante solicitar apenas as informações estritamente necessárias para confirmar quem a pessoa é, minimizando ao máximo a coleta de novos dados pessoais.

2.2 Dos Direitos dos Titulares

Importante que o estabelecimento médico garanta aos titulares o exercício dos direitos previstos na LGPD, sem nenhum custo para o paciente.

Quais são esses direitos? A pergunta é pertinente, em razão da Lei apontar quais são os direitos dos titulares dos dados e a quem eles podem requerer tais ações. Os direitos dos titulares, a seguir desaguam em ações para os Controladores e muitas vezes com suporte dos Operadores de dados. Esmiuçamos cada um deles a seguir:

8. Art. 88. Negar, ao paciente, acesso a seu prontuário, deixar de lhe fornecer cópia quando solicitada, bem como deixar de lhe dar explicações necessárias à sua compreensão, salvo quando ocasionarem riscos ao próprio paciente ou a terceiros.

1. Confirmação da existência de tratamento: é direito do titular saber se os dados dele estão sendo tratados pelo agente, seja ele uma pessoa física ou pessoa jurídica. A resposta aqui deve ser dada dentro de um prazo hábil. Destaque-se que, o referido prazo, segundo a LGPD será dentro de um prazo razoável para que seja atendido tal direito.

2. Acesso aos dados: O controlador de dados pode dispor de meios para que o titular de dados possua condição de saber quais são os seus dados que estão sendo tratados.

3. Retificação: Assim como o acesso aos dados, é necessário que o titular tenha a capacidade de retificar os seus dados, seja de forma automatizada pelo agente de tratamento, seja pela própria ação do titular, por meio de formas disponíveis por estes.

4. Anonimização, bloqueio decorrentes do uso excessivo dos dados dos titulares de dados: É direito dos titulares cobrar dos agentes de tratamento que eles protejam os seus dados através de medidas técnicas de anonimização, criptografia, pseudo anonimização e outras ações decorrentes do *privacy by design*. Ademais, os dados usados além das finalidades dispostas pelos agentes de tratamento de dados devem ser imediatamente descartados.

5. Portabilidade: É direito do titular poder migrar os dados que estão em posse do agente de tratamento para outro agente, dentro de um prazo hábil e sem qualquer retenção de dados do primeiro agente.
A portabilidade dos dados pessoais a que se refere este item não inclui dados que já tenham sido anonimizados pelo controlador.

6. Informação: das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados e informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

7. Revogação do consentimento: Aqui o direito do titular de revogar o consentimento a qualquer tempo dos dados aos quais o agente de tratamento está tratando.

8. Oposição ao tratamento de dados: O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

9. Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses de cumprimento de obrigação legal ou regulatória pelo controlador; estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados[9].

9. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

Disponível aqui

3. Jornada do Paciente na Clínica com foco na privacidade

Naturalmente os titulares de dados costumam ver as informações genéticas sobre si mesmos como privadas de cada pessoa, genoma, ou complemento completo de DNA, é único, estritamente privado. Mas as variantes específicas dentro de um genoma de um indivíduo podem ser amplamente compartilhadas com parentes biológicos ou mesmo com toda a população humana.

Esse caráter misto do genoma – como um conjunto singularmente individual de elementos comuns amplamente compartilhados – o imbui de um duplo significado privado e público que confunde qualquer discussão sobre políticas que abordem a genética privada.
Muitas vezes, adotar as regras dispostas trazidas por uma lei sobre uma situação nova para a clínica, traz inúmeros desafios, seja para os sócios, seja para os funcionários que estão em contato direto com os pacientes. Em algumas situações sem os métodos adequados, tal implementação pode acabar criando certas rusgas entre os pacientes da clínica e o dever desta de atender às obrigações legais, ainda mais na nova configuração de privacidade. Destaque-se que à medida que esta tecnologia e nossa compreensão da genômica melhoraram, um número de indivíduos e entidades buscam acesso à informação genética individual. Por exemplo, milhões de pessoas fizeram testes para aprender sobre seus ancestrais e para identificar parentes antes desconhecidos, empreendimentos que exigem acesso às informações de outras pessoas, bem como às suas próprias. Além disso, os médicos podem buscar os dados para refinar um diagnóstico ou cuidado do paciente. Os pesquisadores biomédicos podem querer examinar as informações genéticas para entender as maneiras pelas quais a variação genética contribui para a saúde e a doença.

As seguradoras com produto de Seguro de Vida podem querer usar essas informações para subscrição. Partes em delito tóxico casos podem tentar usar esta informação para estabelecer ou refutar a causalidade. A aplicação da lei pode querer usar as informações para identificar vítimas de ataques em massa ou crimes suspeitos. Os apontamentos sobre os direitos dos usuários nas clínicas perpassam hoje o exercício da atividade médica, indo além da aplicação de ferramentas digitais, que melhoram o atendimento.

A engenhosidade da tecnologia e o exercício da prática clínica associados podem criar um contexto adequado e transparente para o paciente, tornando a clínica compliance com as práticas de privacidade. Para facilitar a percepção desse comentário é imperioso que a clínica esteja aberta para treinar os seus funcionários em face do uso correto dos dados dos pacientes, seja no momento do mero cadastro dos dados deles para fins administrativos, como também o compartilhamento desses dados com terceiros (operadoras de planos de saúde e outros agentes que recebem os dados oriundos da clínica) e também os dados de saúde dos pacientes que são evoluídos nos prontuários dos estabelecimentos médicos.

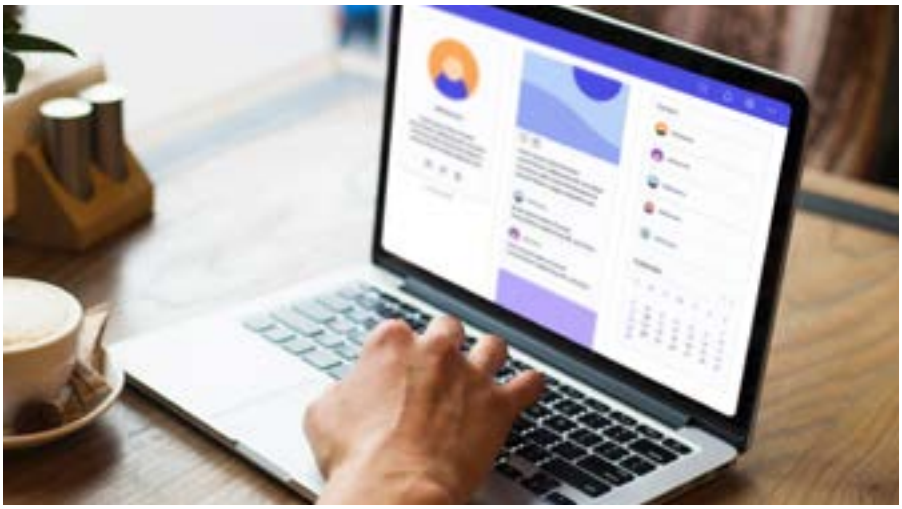
Necessariamente, as pessoas que fazem parte da clínica precisam estar qualificadas em relação aos tratamentos de dados. E como fazer isso? Vamos apresentar um passo a passo que pode ajudar no Compliance as regras da LGPD, a saber:

1. Um dos primeiros passos é capacitar os membros da clínica, sobre as disposições de Privacidade e de Segurança da Informação, aplicado a dados físicos e dados que estejam em plataformas ou softwares. Destaca-se que o maior número de incidentes de vazamento de dados é a falha humana. A falta de treinamento e capacitação dos membros da equipe é um grande porte para eventuais e futuros incidentes de vazamento de dados;

2. É necessário também criar documentos (manuais de orientação de segurança da informação, política de privacidade interna, política de gestão de senhas e orientações de como usar ferramentas de comunicação, tipo WhatsApp Comercial e afins, para evitar a captura de dados indevidos por pessoas não habilitadas para tal; documentos

estes orientativos de como se deve agir com os dados dos pacientes e da equipe, bem como agir em caso de eventual incidente de dados;

3. É preciso reforçar a segurança da rede interna e dividi-la entre um acesso somente para convidados (guests) e a rede interna, apenas para a equipe da clínica, através de uma VPN[10] e a possibilidade de auditar os acessos nos sistemas da clínica, para conseguir identificar em eventuais incidentes de segurança, o agente causador, seja por uma falha tecnológica ou uma falha humana;



4. Outra regra de segurança muito simples e que pode ser muito útil, é a utilização do segundo fator de autenticação para acesso a sistemas integrados à clínica (por exemplo: ferramentas de gestão de prontuários, documentos de gestão de arquivos como Google Drive, Dropbox e outros. A autenticação em dois fatores ou 2FA é o processo de autenticação em que dois dos três possíveis fatores de autenticação são combinados. Os possíveis fatores de autenticação são: algo que o usuário saiba (por exemplo, uma senha, número de identificação pessoal (código PIN) ou resposta a uma pergunta, como também um sequencial de números que fica disponível por um limite de tempo[11]).

5. É necessário criar um inventário de dados, ou seja, um documento que seja possível identificar quais são os dados que são tratados pela Clínica e quem são os responsáveis pela sua coleta. Talvez o diretor da clínica se pergunte, por que tal documento é importante? A lei prioriza este documento? A lei possui uma interpretação de que é necessário que sejam aplicadas ações para que as empresas que tratam dados estejam atendendo o que ela reza. A solicitação do inventário de dados e outros documentos jurídicos como Acordo e Proteção de Dados, Acordo de Confidencialidade, Disposição do atendimento às regras da LGPD devem ser comprovados através de documentos e não somente ações.

6. Outro fator importante é a revisão dos contratos com terceiros para verificar se estão atendendo também às disposições legais das

10. VPN significa "Virtual Private Network" (Rede Privada Virtual) e descreve a oportunidade de estabelecer uma conexão de rede protegida ao usar redes públicas. As VPNs criptografam seu tráfego de Internet e disfarçam sua identidade online.

11. www.onespan.com

normas de privacidade. Normalmente as clínicas dependem de terceiros para algumas ações pontuais, como realização de exames, contabilidade, jurídico, ferramentas para a gestão de prontuários, ferramentas para prescrição de medicamentos, ferramentas para realização de telemedicina, tele orientações e afins;

7. É imperioso também criar orientação de como proceder em caso de incidentes que resultem em vazamento de dados dos pacientes da clínica, pois, ocorrendo tal fato, é necessário que haja uma rotina para minimizar os danos e identificar a causa do incidente. A Lei preconiza um plano de incidentes onde cada membro saiba como agir para evitar uma propagação indevida dos dados de saúde;

8. Destaca-se que todas estas ações também devem refletir para os pacientes da clínica. Pois eles precisam saber os seus direitos em face do uso dos seus dados. E como fazer isso? A clínica pode apresentar a eles a Política de Privacidade, documento que mostrará quais dados serão coletados e tratados para as devidas finalidades, com quem será compartilhado e por que razão permanecerão na base de dados da clínica. Além disso, os pacientes precisam saber como devem encaminhar exames e proceder em diálogos em ferramentas de conversação, como WhatsApp comercial e afins. Tudo isso pode ser feito através de orientações ou as chamadas privacy notices, ações comunicativas diretas para o paciente, seja no ambiente físico da clínica seja no ambiente virtual, cuja função é orientar e evitar incidentes de dados.

Algumas das ações acima serão detalhadas nos itens no decorrer do texto para facilitar a sua compreensão e entender melhor como será dará a exequibilidade de tal ação. Cada etapa é importante para atender aos critérios das regras de privacy by design na sua clínica. Para cada etapa da jornada do usuário (paciente) observa-se a necessidade da clínica adotar medidas pontuais de privacidade.

No dia a dia da clínica é que se observa o desenvolvimento da captura das informações estritamente necessárias para realizar o tratamento do paciente e não o expor para os demais pacientes que se encontram no local de espera. Pensar em uma exposição mínima e comunicação direta com o paciente sobre a forma de tratamento dos seus dados já será um grande diferencial para tornar a sua clínica privacy by desing[12].

Para as clínicas, é necessário pontuar a importância de informar a seu paciente de que os seus dados são tratados para uma finalidade

12. Privacy by design é um conceito de abordagem à Engenharia de Sistemas, a qual leva em conta a privacidade durante todo o processo de construção do software ou do serviço prestado. É um conceito sensível aos vetores humanos e todas as suas derivações em todo o processo. O conceito surgiu durante o relatório conjunto "Privacy-enhancing technologies" de um time formado pelo Ïnformation and Privacy Commissioner" de Ontário, Canadá, o "Dutch Data Protection Authority". O desenvolvimento de tal técnica foi criada pela Canadense Ann Cavoukian.

Disponível aqui

específica (tutela à saúde) e que, caso necessário, serão compartilhados com terceiros para dar continuidade ao tratamento. Além da informação apontada pelo atendente ou recepcionista, é importante, no contexto atual, disponibilizar para os pacientes, no formato de pequenos cartazes, ou até mesmo orientações específicas nas telas sobre privacidade, o que chamamos tecnicamente de privacy notices. É importante destacar que a linguagem deve ser clara e acessível, que não gere dúvidas ao usuário. Notadamente, como informa a Lei Geral de Proteção de Dados, os dados de saúde são qualificados como dados sensíveis, ou seja, são dados que, por sua natureza, podem vir a gerar alguma discriminação em razão da condição de saúde, e outros elementos descritos na referida lei. A própria traz um dispositivo que impede operadoras de saúde de usarem dados do paciente de forma discriminatória (por exemplo: cobrar mais daquelas pessoas que podem adoecer mais ou que possuem um estilo de vida pouco saudável).

Bem, sabendo que os dados tratados pela clínica são dados sensíveis, devemos observar que a base legal para o seu tratamento é, regra geral, o consentimento, ou seja a manifestação voluntária, livre, informada e inequívoca e incluir a garantia do opt-out[13] a qualquer momento. Estruturado como um documento claro e direto, o consentimento apontado na LGPD é a forma mais usual, mas não menos complexa, para que se consiga tratar os dados do paciente. O período de experiência, como aponta no quadro, aponta algumas ideias de como pensar na adequação da clínica. As formas são diversas, pois a clínica tendo entrada ou não nas mídias digitais pode apontar algumas das opções para informar o paciente do tratamento dos seus dados e ainda levantar informações através de FAQ.

3.1 Da possibilidade de envio de dados dos pacientes para Operadoras de Saúde:

O tratamento de dados pessoais sensíveis somente poderá ocorrer: com consentimento que evidencie uma manifestação livre, informada e inequívoca, e destacado para finalidades específicas do titular ou seu responsável legal. No caso de compartilhamento com operadoras de planos de saúde, a base legal poderá ser o cumprimento de obrigação legal ou mesmo a execução de um contrato.

Há situações em que o consentimento do titular pode ser dispensável, segundo previsão do art. II: "tutela da saúde exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária". Importante o disposto no §5°: "É vedado às operadoras de planos privados de assistência à saúde, o tratamento de dados de saúde para prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

13. É a possibilidade de o paciente (usuário) se descadastrar da agregação de dados e das análises sobre a visita ou atendimento daquele na clínica.

3.2 Da Necessidade de treinamento de colaboradores:

É bastante comum que médicos compartilhem com suas secretárias as senhas de prontuários eletrônicos. Ou ainda que, sendo prontuários físicos, a secretária tenha acesso direto a dados sensíveis ali registrados e que, se vazados, resultam em sérias consequências ao médico. Colaboradores assumem um importante papel na proteção de dados e devem ser treinados, capacitados, para garantirem o direito à privacidade dos titulares, bem como a observância de todos os direitos dos titulares. Necessário incluir uma Cláusula de Confidencialidade no Contrato de Trabalho dos colaboradores para que se torne uma obrigação contratual com a Clínica.

Auxiliares e até outros médicos deverão estar atentos para discussões de casos, algumas vezes inclusive na presença de outros pacientes. Mas, a cena é bastante comum em corredores de clínicas e hospitais. Diante dos apontamentos acima, vamos aplicar agora os preceitos práticos para adoção nas clínicas.

Ademais, acrescente-se que é necessário que as referidas ações estejam refletidas no contrato de trabalho, como cláusula de confidencialidade e cláusulas de privacidade também. Tais cláusulas podem ser inseridas no contrato de trabalho ou de prestação de serviços ou podem vir de forma anexa em um documento próprio, como um Acordo de Confidencialidade e Acordo de Proteção de Dados. Confira a seguir uma ideia de cláusula sobre o tema em questão:

Não tratar Dados Pessoais sem propósito e finalidade específica e de forma diferente do estipulado e definido pela Clínica, desnecessários e inadequados para execução da Parceria e/ou contratos firmados com clientes finais, a não ser que sejam essenciais ao cumprimento do contrato/parceria, como exemplo: ID do colaborador, empresa e saldo disponível para saque, entre outros.

3.3 Exemplos práticos:

Que medidas de privacidade adotadas devem ser aplicadas para marcar uma consulta?

• Limite sobre as informações coletadas pela clínica;
• Informar ao paciente que a clínica garante que seus direitos sejam respeitados;
• Informar a política de privacidade da clínica;
• Disponibilizar na clínica *Privacy Notices*.

Que obrigações devemos adotar?

Quando as consultas são marcadas, os dados pessoais de seus pacientes são coletados, registrados e usados, em particular sua identidade e detalhes de contatos pessoais. Às vezes, os motivos da consulta podem ser solicitados com um grau de precisão que varia de acordo com as especialidades e as necessidades de preparação para um exame específico. Essas informações podem fornecer informações sobre o estado de saúde do paciente, assim como o conhecimento de uma consulta com um especialista pode fornecer uma indicação do estado de saúde (por exemplo, consultar um cardiologista regularmente).

Destaque-se que aqui é possível solicitar algumas informações dos pacientes através de um questionário pré-consulta ou mesmo a Anamnese enviados de forma criptografada (ou por email, com segurança) para que ele possa já encaminhar algumas informações relevantes para a jornada dele na clínica, sem que tais dados passem pelos colaboradores.

Atenção! Ao contrário de prontuários de "pacientes", que têm um período de retenção longo, os dados relacionados à marcação de compromissos podem ser excluídos quando não forem mais necessários. Essa duração deve ser pensada de acordo com a sua atividade, sabendo que as datas dos exames e consultas médicas são, em qualquer caso, registradas nos arquivos de seus pacientes.

3.4 Que medidas devem ser tomadas para preservar a privacidade do prontuário dos pacientes?

1. Limitar as informações coletadas necessárias e uso dos arquivos dos pacientes de acordo com os objetivos bem definidos (monitoramento dos pacientes);

2. Excluir os arquivos de pacientes sobre alguma informação que tenha excedido o período de retenção recomendado, pelo Código de Ética Médica e pela Lei do Prontuário. Estabelecer medidas de segurança apropriadas para o arquivo de pacientes. Por exemplo, se os prontuários forem físicos, é necessário ter um sala com chave ou arquivos com cadeados. Se eletrônicos, criar uma gestão de senhas fortes, aplicar fato de dupla verificação, bem como VPN para acesso a tais dados e outras ações que restrinjam os acessos de pessoas má intencionadas.

3. A clínica deve garantir que o uso de registros de "pacientes" respeite os princípios fundamentais da proteção de dados pessoais.

No dia a dia da prática profissional, a clínica usa o software fornecido por um provedor de serviços de TI para manter os arquivos do paciente ou mantém os arquivos "pacientes" em formato de papel. Esses arquivos necessariamente contêm dados pessoais de seus pacientes e outros profissionais de saúde envolvidos no acompanhamento. Portanto, você é considerado "responsável de tratamento", na acepção dos regulamentos sobre proteção de dados pessoais. A clínica deve garantir que os arquivos estejam em conformidade com a LGPD.

Se o prontuário é físico (em papel) ou algum software médico administrativo, como a clínica deve proceder?

• De antemão, sendo o arquivo de papel ou algum software, deve atender a propósitos específicos, explícitos e legítimo. Tais como: preservá-los em locais de difícil acesso para terceiros.

• As informações coletadas nos arquivos dos pacientes são usadas para exercer sua atividade de prevenção, diagnóstico e assistência e são usadas para gerenciar sua prática. eles atendem às necessidades de atendimento de seus pacientes.

• Ao usar estas informações é importante observar com atenção o gerenciamento das consultas; gerenciamento dos prontuários médicos; realização das prescrições; envio de e-mails aos colegas; estabelecimento e transmissão remota de informações sobre o tratamento.

Qualquer outro uso das informações coletadas deve ser feito com cuidado. Em particular, qualquer uso pessoal ou comercial dos dados dos pacientes é proibido pela LGPD. Para que a clínica consiga usar estes dados para outra finalidade ela precisa providenciar a anuência a novo termo de consentimento.

3.5 O que deve ser excluído do prontuário do paciente?

Qualquer informação não relacionada ao assunto da consulta do paciente ou que não seja essencial para o diagnóstico ou a prestação de cuidados deve ser excluída. Exemplo: não é relevante coletar dados sobre informações da vida privada do paciente que não sejam clinicamente necessários (por exemplo: time pelo qual ele torce, informação financeira, orientação filosófica ou política, etc).

3.6 Por quanto tempo a clínica deve armazenar os dados?

É importante levar em consideração os prazos de prescrição para quaisquer ações de responsabilidade e/ ou disposições especiais.

Afastada a informação quanto às questões de responsabilidade é imperioso destacar o que é informado na legislação específica sobre o tema de armazenamento de prontuário. A saber: 20 anos a partir da data da última consulta do paciente;

• Se o paciente for menor de idade e esse período de 20 anos expirar antes de 28 anos, o armazenamento de informações a seu respeito deve ser estendido até essa data;

• Em todos os casos, se o paciente morrer menos de 10 anos após sua última consulta, as informações a seu respeito deverão ser mantidas por 10 anos a partir da data da morte;

3.7 A clínica deve informar aos pacientes sobre a existência de seus registros e direitos sobre proteção de dados e privacidade ? (privacy notices).

As informações podem ser feitas por postagem, na sala de espera e/ou pela entrega de um documento específico (exemplo: folheto entregue ao paciente ou disponibilizado na sala de espera).

As referidas informações devem incluir os seguintes elementos:
• nome do diretor clínico e o do encarregado de dados e os respectivos e-mails do diretor técnico e/ou do DPO e detalhes de contato;
• os propósitos e a base legal do tratamento, incluindo propósitos subsequentes;
• destinatários dos dados;
• prazo de conservação.
• direitos da pessoa: acesso, retificação, exclusão sob certas condições, limitação, oposição;
• natureza obrigatória dos dados fornecidos e as possíveis consequências de uma falha na resposta.

Seus pacientes têm direitos e eles podem:
• acessar dados sobre eles;
• solicitar a retificação desses dados no caso de algum erro;
• opor-se ao processamento por razões relacionadas a uma situação específica;
• apagar os dados em determinadas situações específicas (arquivo do paciente mantido por muito tempo acima do previsto na legislação ou dados não adequados, por exemplo).

Cada solicitação acima deve ser examinada dentro de um prazo razoável, por exemplo até 15 dias.

3.7.1 Há obrigatoriedade de apresentar a política de privacidade e os termos de uso para o paciente? Em que momento?

A política de privacidade, termos de uso e as privacy notice sempre devem estar acessíveis ao paciente. Tanto a política de privacidade quanto os termos de uso são documentos obrigatórios e devem ser passados ao paciente no momento de pré-experiência, ou seja, antes mesmo da consulta presencial ou a distância. Ou seja, no momento de realização do cadastro ou até mesmo pelo site da clínica, estando disponíveis sempre que solicitado. Já as privacy notices devem ser uma interação visual com o paciente, sempre disponíveis e refletindo o que os outros documentos citados abarcam.

A jornada do usuário deve atender os princípios da finalidade, adequação, necessidade, segurança, não discriminação, entre outros propostos na LGPD.

3.7.2 Sobre o uso do whatsapp em consultórios e a questão da privacidade

Sem dúvida, na relação médico e paciente, o WhatsApp tem sido uma ferramenta facilitadora. Não obstante essa facilidade pode ensejar um incidente de segurança, o que, aliás, já ocorreu inclusive de forma amplamente divulgada pela mídia.

O uso do WhatsApp está regulamentado pelo Conselho Federal de Medicina em parecer específico cuja ementa assevera que é "permitido o uso do WhatsApp e plataformas similares para comunicação entre médicos e seus pacientes, bem como entre médicos e médicos, em caráter privativo, para enviar dados ou tirar dúvidas, bem como em grupos fechados de especialistas ou do corpo clínico de uma instituição ou cátedra, com a ressalva de que todas as informações passadas tem absoluto caráter confidencial e não podem extrapolar os limites do próprio grupo, nem tampouco podem circular em grupos recreativos, mesmo que composto apenas por médicos."

Também se extrai de parecer do Conselho Federal de Medicina (Parecer-Consulta 14/2017 CFM[14]) que a troca de informações entre pacientes e médicos, quando se tratar de pessoas já recebendo assistência, é permitida para elucidar dúvidas, tratar de aspectos evolutivos e passar orientações ou intervenções de caráter emergencial. Se relevante, deve orientar o paciente a comparecer ao consultório e registrar em pron-

14. sistemas.cfm.org.br/normas

tuário ou ficha clínica, no primeiro momento em que o médico tiver acesso ao mesmo. Ainda que haja permissão para tal uso, a ferramenta não foi concebida para a troca de dados sensíveis, como são aqueles que envolvem a saúde do paciente, salvo se for essencial e urgente. Também não se trata de uma ferramenta segura, ainda que haja criptografia de ponta a ponta, é fato que há permissão para compartilhamento de informações sem qualquer filtro ou dificuldade, basta que se use a função "encaminhar".

Ademais, os smartphones permitem prints de tela que podem ser enviados por qualquer via e serem usados de maneira indevida e prejudicial ao paciente. Com foco na privacidade, o melhor é utilizar essa ferramenta somente para orientações gerais, marcação de consultas, sempre com celular institucional destinado somente ao fim de comunicação com os pacientes.

Em certos consultórios, ocorre que pacientes encaminham fotos pessoais (identificadas) para celulares que ficam sob os cuidados das secretárias. Essa prática não é compliance à LGPD, pois torna os dados pessoais vulneráveis à ocorrência de um incidente de segurança. Por fim, devemos lembrar que, em caso de orientação ao paciente, de forma assíncrona principalmente, corre-se o risco de uma interpretação inadequada por parte de quem lê a mensagem e acrescente-se o agravante de eventual uso do corretor ortográfico que modificaria o conteúdo. Outra questão não menos relevante: como precificar esse tempo gasto para responder aos pacientes? Se o profissional conseguir incorporar a hora técnica utilizada para avaliar a dúvida do paciente e a resposta efetiva da resposta médica, poderá ser menos gravosa à utilização, quanto ao quesito remuneração.

Hoje conversas de WhatsApp têm sido usadas como prova em casos de judicialização. Desta forma, se você quer minimizar os riscos de problemas, sugerimos optar por outra ferramenta, em especial no que se refere ao uso do chat.

4. Mais sobre Telemedicina e privacidade

No mundo a Telemedicina já é prática rotineira. Em outubro de 1999, o conceito de Telemedicina, bem como seus princípios e responsabilidades, foram editados em um documento chamado Declaração de Tel Aviv[15], que trata das normas éticas na utilização da telemedicina. Como princípios universais e norteadores da prática médica destacamos os princípios da beneficência e da não maleficência.
Nesse esteira, incluímos o Art. 2° do Capítulo I - dos Princípios Fundamentais - do Código de Ética Médica:

"O alvo de toda a atenção do médico é a saúde do ser humano, em benefício da qual deverá agir com o máximo de zelo e o melhor de sua capacidade profissional."

Em relação à Telemedicina, a necessidade de tratamento de grandes volumes de dados sensíveis (dados cadastrais de pacientes, queixas de saúde, antecedentes, histórico de doenças, pedidos e resultados de exames, hipóteses diagnósticas, plano terapêutico, evolução clínica e pareceres, dentre outros) torna a LGPD objeto de interesse.
Lembre-se de que nesses serviços prestados por telemedicina (teleconsulta, telorientaçao, telemonitoramento, telecirurgia, teleinterconsulta), os dados e imagens dos pacientes irão trafegar na rede mundial de computadores (internet). A plataforma escolhida sempre será responsabilidade do médico, de forma que é essencial garantir que haja infraestrutura, gerenciamento de riscos e requisitos obrigatórios para assegurar o registro digital apropriado e seguro. O texto da Resolução CFM 2314/2022 dispõe que o médico deverá escolher uma Sistema

15. www.dhnet.org.br

de Registro Eletrônico em Saúde que apresente NGS2; em tese, o fornecedor do sistema de prontuário eletrônico adotado com uma plataforma integrada para a telemedicina deveria ter a certificação fornecida pela SBIS (Sociedade Brasileira de Informática em Saúde) ou garantir ao médico que foram observados todos os requisitos presentes no manual de certificação da SBCIS[16].

No momento de avanço da Telemedicina no país, também se destaca o Projeto de lei[17] aprovado na Câmara dos deputados. A referência à LGPD, assim como ocorre na Resolução 2134/2022, se faz presente. Portanto, não se trata de uma faculdade a adequação à lei, mas sim é um imperativo legal e ético. Destaca-se do texto do Projeto de Lei:

Art. 6º A prática da telemedicina deve seguir as seguintes determinações:
2. obediência aos ditames das Leis nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet) e nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados).
Outro cuidado está relacionado ao Termo de Consentimento a ser apresentado ao paciente para que, por meio de informações claras e objetivas, ele esteja ciente das particularidades que envolvem a telemedicina em especial naquilo que se refere à privacidade e à proteção dos dados. O referido PL 1998/20 aponta para o seguinte trecho:

1. ser realizada por livre decisão do paciente, ou de seu representante legal, e sob responsabilidade profissional do médico;
A Resolução 2134/2022 aponta para a necessidade de se observar a autonomia do paciente, o qual somente poderá exercê-la se compreender riscos e benefícios que envolvem a utilização dessa metodologia. A vulnerabilidade da segurança de dados é um dos riscos, portanto, necessariamente deverá constar no Termo de Consentimento essa informação para que o paciente possa concordar ou discordar da utilização da telemedicina:

Art. 15. O paciente ou seu representante legal deverá autorizar o atendimento por telemedicina e a transmissão das suas imagens e dados por meio de (termo de concordância e autorização) consentimento, livre e esclarecido, enviado por meios eletrônicos ou de gravação de leitura do texto com a concordância, devendo fazer parte do SRES do paciente.

Parágrafo único. Em todo atendimento por telemedicina deve ser assegurado do consentimento explícito, no qual o paciente ou seu representante legal deve estar consciente de que suas informações pessoais podem ser compartilhadas e sobre o seu direito de negar permissão para isso, salvo em situação de emergência médica.

Vale ressaltar que o Código de Ética Médica traz a seguinte disposição sobre a obrigatoriedade do uso do Termo de Consentimento[18]:

16. sbis.org.br

17. www.camara.leg.br

18. O Manual apresenta como anexo modelos de Termos de Consentimento.

Art. 22. Deixar de obter consentimento do paciente ou de seu representante legal após esclarecê-lo sobre o procedimento a ser realizado, salvo em caso de risco iminente de morte.

Por se tratar a telemedicina de uma outra metodologia, cabe sim ao profissional médico esclarecer suas características próprias se comparadas a uma consulta presencial.

Ainda sobre o tema, o CDC (Código de Defesa do Consumidor)[19] dispõe, em seu Art. 6°, inciso III:

Art. 6° São direitos básicos do consumidor:

3. a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade e preço, bem como sobre os riscos que apresentem;
Importância do uso do certificado Digital para as prescrições eletrônicas (ou outro legalmente aceito). Um dos passos importantes relacionados a realização de uma teleconsulta está no momento da prescrição dos medicamentos.

Sobre e emissão de documentos médicos, já se citou aqui nesse texto (para corroborar a necessária adesão da plataforma utilizada à LGPD,), ter o Conselho Federal de Medicina emanado regulamento específico:
A Resolução 2199/2021 (sobre emissão de documentos eletrônicos) apresenta em seu artigo:

Art. 4° A emissão de documentos médicos por meio de TDICs deverá ser feita mediante o uso de assinatura digital, gerada por meio de certificados e chaves emitidos pela Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil), com Nível de Garantia de Segurança 2 (NGS2), garantindo sua validade legal, autenticidade, confiabilidade, autoria e não repúdio. Parágrafo único. Os documentos médicos devem possibilitar reconhecimento da assinatura digital por serviços de validação do Instituto Nacional de Tecnologia da Informação (ITI) ou por validador disponibilizado pelo CFM.

Por que se faz importante o uso de um Certificado Digital, em especial quando se fala aqui de direitos dos titulares, consoante nomenclatura utilizada no texto da LGPD? Porque através do Certificado Digital garante-se a identidade virtual do médico, o que traz segurança para o paciente. Os tipos de medicamentos que podem ser prescritos eletronicamente são definidos pela ANVISA[20].

Dessa forma, em 2 de março de 2020, a Anvisa emitiu a Nota Técnica n°31, que informa sobre a possibilidade de utilização de assinatura digital em receituário de medicamento sujeito a controle especial, conforme a seguir (BRASIL, 2020): 7. *No que se refere a prescrições de medicamentos sujeitos a controle especial, essa possibilidade somente se aplica a Receitas de Controle Especial, utilizada para medicamentos que*

19. presrepublica.jusbrasil.com.br

20. www.crfsp.org.br

contenham substâncias da Lista C1 e C5 e dos adendos das Listas A1, A2 e B1 da Portaria SVS/MS nº 344/98, desde que também sejam atendidas todas as exigências previstas na legislação sanitária. Destarte, a assinatura digital também pode ser aplicável à prescrição de medicamentos antimicrobianos. A Resolução 2134/2022 , em seus "considerandos" (que representam a fundamentação da Resolução) apresenta a exigência de que o médico tenho o certificado digital, exatamente como forma de garantir a sua identidade e dar ao paciente segurança jurídica: *CONSIDERANDO que, para atuar por telemedicina, o médico deve possuir assinatura digital qualificada, padrão ICP-Brasil, nos termos das Leis vigentes no país;*

Essas exigências fundamentam-se também na necessidade de proteção de dados; afinal, comprovar a autenticidade do médico nos documentos emitidos é uma forma de se proteger os dados para que não sejam utilizados por aqueles que não tem obrigação de sigilo profissional. Desta forma, é possível minimizar os riscos seguindo as recomendações aqui expressas, tendo ciência, porém, que a adequação à LGPD é um processo complexo, que há documentos que são obrigatórios e que o trabalho é constante. Por isso, inclusive, seria importante nomear um profissional responsável por aplicar a Política de Proteção de Dados e Segurança da Informação criada pela clínica.


SBGM
Sociedade Brasileira
de Genética Médica
e Genômica