LATINI GROUP
Integrated
Business
Solution

Av. Vereador José Diniz, 2.270
São Paulo ● SP ● Brasil/ Brazil
CEP/ Zipcode: 04604-003
Tel./ Phone: 55 11 5090 5080
Fax: 55 11 5090 5083
Site: www.latinigroup.com

A ANVISA E A CIBERSEGURANÇA DOS DISPOSITIVOS MÉDICOS

Um fenômeno que ocorre em todo o mundo é a questão de a tecnologia sempre avançar mais rapidamente do que as leis e os marcos regulatórios. Enquanto as leis deveriam ser o reflexo do mundo em que vivemos, do momento da sociedade, regrando as relações pessoais, de consumo e outras, os marcos regulatórios são conjuntos de normas, regulamentos e resoluções que estabelecem as regras e diretrizes para a fabricação, comercialização, importação, distribuição e uso de produtos sujeitos à sua regulamentação. Esse cenário no qual a tecnologia sempre avança mais rápido do que a legislação e a regulamentação, é de se esperar que muitos assuntos fiquem de fora da agenda regulatória e dos marcos regulatórios já estabelecidos, tornando-se alvos de medidas intercorrentes até que os marcos regulatórios definitivos sejam aprovados e publicados, seguindo-se o rito legal. A questão da cibersegurança não recebeu tratamento diferente. Com o rápido a avolumado avanço das tecnologias médicas, surgiu a preocupação com a integridade dos dados, acessos inadequados ou não autorizados, possibilidades de "hackeamento" e da segurança de pacientes e usuários. No Brasil, temos a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD)[1], a qual versa basicamente sobre o tratamento de dados pessoais, entre ela os chamados "dados sensíveis"[2], ou seja, aqueles que fazem referência, entre outros, sobre dados referentes à saúde, que é o tema de abrangência da Agência Nacional de Vigilância Sanitária (ANVISA). Para que o assunto pudesse ser tratado já de forma técnica, porém ainda não sob a égide de uma Resolução de Diretoria Colegiada (RDC) ou Instrução Normativa (IN), a ANVISA fez publicar, em 2020, o Guia nº 38/2020[3] denominado Princípios e Práticas de Cibersegurança em Dispositivos Médicos. O Guia nº 38/2020 encontra a sua base legal no Art. 12 da Lei nº 6360/1976[4], no Art. 8º da Lei nº 9.782/1999[5] e da RDC nº 185/2001 (substituída posteriormente pela RDC nº 751/2022[6]). O texto do referido Guia traz recomendações para os fabricantes dos dispositivos médicos, porém de adoção voluntária. O documento ainda não tem caráter impositivo. O escopo desse documento é a **garantia da manutenção e continuidade da segurança do paciente e desempenho do dispositivo**. Em outras palavras, a preocupação da ANVISA em relação ao tema da cibersegurança, é a segurança do paciente, alvo final de todas as ações em vigilância sanitária, bem como a continuidade do correto funcionamento dos dispositivos médicos, o principal item de análise por parte da ANVISA quando da análise regulatória dos processos de notificação ou registro dos produtos. Apesar do documento ser dirigido aos fabricantes de dispositivos médicos, lembramos que os importadores e distribuidores são tão responsáveis quanto os fabricantes quando o tema é a segurança e a eficácia dos produtos, além da responsabilidade sobre o fato do produto. Tal isonomia de responsabilidades veio à lúmen com a publicação do Código de Defesa do Consumidor[7], como segue:

> Art. 12. *o fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou*

[1] https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
[2] II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural
[3] https://www.gov.br/anvisa/pt-br/assuntos/noticias-anvisa/2020/saiba-mais-sobre-cibersegurança-em-dispositivos-medicos/guia-38.pdf
[4] https://www.planalto.gov.br/ccivil_03/leis/l6360.htm
[5] https://www.planalto.gov.br/ccivil_03/leis/l9782.htm
[6] https://www.in.gov.br/en/web/dou/-/resolucao-rdc-n-751-de-15-de-setembro-de-2022-430797145
[7] https://www2.senado.leg.br/bdsf/bitstream/handle/id/496457/000970346.pdf

Av. Vereador José Diniz, 2.270
São Paulo ● SP ● Brasil/ Brazil
CEP/ Zipcode: 04604-003
Tel./ Phone: 55 11 5090 5080
Fax: 55 11 5090 5083
Site: www.latinigroup.com

acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos.

Portanto, não é argumento plausível a ser utilizado pelo importador / distribuidor, alegar a não responsabilidade sobre o fato do produto. O próprio texto da lei determina que este responderá "independentemente de culpa", assim como o fabricante local.

Ainda no capítulo das Responsabilidades, frise-se que, conforme o critério documentado pela ANVISA no guia, "**os intervenientes têm responsabilidade compartilhada em relação à cibersegurança de dispositivos médicos**". Na prática, isso quer dizer que cabe a cada player, se responsabilizar pela sua parcela no uso e manutenção da segurança dos dispositivos. Por exemplo, se um fabricante desenvolveu o dispositivo médico de forma adequada, observando as normas e regulamentos aplicáveis, mas o hospital ou o profissional de saúde o instalou ou o está operando de forma a permitir a redução ou quebra da cibersegurança e, se isso acarretar danos ao paciente, então será de responsabilidade desse player arcar com as consequências de sua ação ou omissão. Aqui vale a pena abrir um parênteses na conversa e frisar que o tremo "Responsabilidade Compartilhada" também se aplica à gestão dos resíduos sólidos, entre eles os dispositivos médicos, da acordo com o Art. 3º, XVII, da Lei nº 12.305/20108.

Sob a ótica do Guia nº 38/202, da ANVISA, o importador é tão responsável pelo tema da cibersegurança quanto o fabricante brasileiro, embora o primeiro não participe das fases de projeto, qualificação e montagem dos dispositivos médicos. Cabe, nesta parte deste breve artigo, lembrar que quando nos referimos a dispositivos médicos, no tema em pauta, estamos discorrendo sobre equipamentos que funcionam com base em softwares, ou seja, os "firmwares" (p.ex. equipamentos de ultrassom, ressonâncias magnéticas, bombas de infusão e monitores miltiparamétricos, entre outros) ou podemos estar nos referindo aos softwares como produtos para saúde (SaMD – Softwares as Medica Devices) ou os softwares médicos utilizados em plataformas online (nuvem) como os Saas – Software as a Service. A RDC nº 657/2022[9] disciplina o tema dos softwares médicos e informa a quais produtos tal definição não se aplica, a saber:

I - para bem-estar;
II - relacionado em lista disponibilizada pela Agência Nacional de Vigilância Sanitária (Anvisa) de produtos não regulados;
III - utilizado exclusivamente para gerenciamento administrativo e financeiro em serviço de saúde;
IV - que processa dados médicos demográficos e epidemiológicos, sem qualquer finalidade clínica diagnóstica ou terapêutica; e
V - embarcado em dispositivo médico sob regime de vigilância sanitária.

Para este último, vale ressaltar que, uma vez notificado ou registrado o dispositivo médico, o software que o acompanha também estará automaticamente regularizado no Sistema Nacional de Vigilância Sanitária. Isso porque vale o conceito de "firmware" supramencionado, ou seja, o hardware não funciona sem o software e vice-versa.

[8] https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/lei/l12305.htm

[9] https://www.in.gov.br/en/web/dou/-/resolucao-de-diretoria-colegiada-rdc-n-657-de-24-de-marco-de-2022-389603457

Av. Vereador José Diniz, 2.270
São Paulo ● SP ● Brasil/ Brazil
CEP/ Zipcode: 04604-003
Tel./ Phone: 55 11 5090 5080
Fax: 55 11 5090 5083
Site: www.latinigroup.com

O tema da cibersegurança, sob a ótima de segurança do paciente e da manutenção do correto funcionamento dos dispositivos médicos, é um requisito a ser considerado pelos fabricantes, desde a fase das variáveis de entrada de projeto até a fase de pós-comercialização, ou seja, a chamada Tecnovigilância, e ao fim do suporte (*end of Support – EOS*, em inglês). No Guia nº 38/2020, a ANVISA não só aborda o tema de forma iminentemente técnica indicando uma série de normas e regulamentos a serem observados (lembrando que a adoção do guia é voluntária e não impositiva) como também trata de incentivar a participação das empresas em fóruns específicos, visando o compartilhamento das informações sobre incidentes, ameaças e vulnerabilidade, além de dar transparência aos dados obtidos. Certamente, tal compartilhamento fortalecerá a segurança do paciente como um todo, haja vista acelerar a velocidade de aprendizado e a adoção das medidas necessárias para um melhor desempenho e proteção dos dispositivos médicos.

Quando falamos em cibersegurança voltada ao paciente e aos usuários, temos que trazer à tona o conceito de **Dano**, sob a ótica regulatória da Vigilância Sanitária. Para tanto, apelamos à RDC nº 36/2013[10], a qual versa sobre ações para a segurança do paciente em serviços de saúde, bem como ao Relatório Técnico da Organização Mundial da Saúde (OMS) de 2009[11]:

> *Art. 3º Para efeito desta Resolução [RDC nº 36/2013] são adotadas as seguintes definições:*
>
> *III - dano: comprometimento da estrutura ou função do corpo e/ou qualquer efeito dele oriundo, incluindo doenças, lesão, sofrimento, morte, incapacidade ou disfunção, podendo, assim, ser físico, social ou psicológico.*

O gerenciamento de riscos deve ser planejado e incorporado de tal forma a permitir o perfeito funcionamento e segurança ao longo de todo o ciclo de vida do produto (*Total Life Cycle – TLC*, em inglês), uma vez que o risco na cibersegurança pode afetar desde os dados utilizados no diagnóstico, até a fase de implementação da terapêutica adequada, conforme a norma ISO 14971:2019. O fabricante pode se valer de ferramentas e abordagens para proceder à modelagem das ameaças, danos ao paciente, mitigações dos riscos e testes de segurança avaliações de risco, como por exemplo:

1. Avaliação de riscos de segurança;
2. Modelagem de ameaças e;
3. Pontuação de vulnerabilidades.

A simulação de ataques, o ambiente onde o dispositivo médico será utilizado, a busca por vulnerabilidades conhecidas e as análises técnicas de segurança são itens que devem compor a cesta de ferramentas e soluções adotadas pelos fabricantes. Obviamente, uma vez comercializados os dispositivos médicos, cabe aos fabricantes, importadores e usuários o constante e proativo monitoramento do ambiente de uso afim de detectar e identificar novas vulnerabilidades e tomar as medidas que elevem o grau de proteção dos pacientes, evitando danos ao mesmo e mantendo o grau de segurança e eficácia dos produtos. Isso deve se manter por todo o período de vida útil do dispositivo médico, uma vez que o surgimento de novas ameaças é constante e dinâmico. Como mencionado, incentiva-se o compartilhamento das informações, não somente em fóruns

[10] https://bvsms.saude.gov.br/bvs/saudelegis/anvisa/2013/rdc0036_25_07_2013.html
[11] https://bvsms.saude.gov.br/bvs/publicacoes/documento_referencia_programa_nacional_seguranca.pdf

Av. Vereador José Diniz, 2.270
São Paulo ● SP ● Brasil/ Brazil
CEP/ Zipcode: 04604-003
Tel./ Phone: 55 11 5090 5080
Fax: 55 11 5090 5083
Site: www.latinigroup.com

específicos, mas principalmente com as autoridades regulatórias, na figura da ANVISA ou de outras nacionalidades com o intuito de permear tais informações com vistas à prevenção e correção de ameaças e problemas, preservando-se a segurança do paciente e evitando-se problemas aos demais intervenientes (stakeholders).

Uma vez pronto para a comercialização, o produto deve vir sempre acompanhado de rotulagem e instruções de uso / manual do usuário com informações claras e precisas, como preconiza a legislação sanitária e o próprio Código de Defesa do Consumidor, abaixo:

> *SEÇÃO II*
> *Da Oferta*
> *Art. 31. A oferta e apresentação de produtos ou serviços devem assegurar* ***informações corretas****, claras, precisas, ostensivas e em* ***língua portuguesa*** *sobre suas características, qualidades, quantidade, composição, preço, garantia, prazos de validade e origem, entre outros dados, bem como sobre os riscos que apresentam à saúde e segurança dos consumidores.*

Além dos itens já citados, como dispositivo médico, o software médico, seja ele SaMD ou SaaS, está sujeito a todas as demais legislações aplicáveis a produtos dessa categoria, como o Código Civil, Código Penal, Código Tributário, Lei Geral de Proteção de Dados, etc.

Resumindo, o tema da Cibersegurança para dispositivos médicos é um assunto complexo e altamente técnico que requer a estrita observância das normas aplicáveis e constante monitoração por parte do fabricante ou do importador. Certamente esse é um tema que evoluirá sob a ótica regulatória, com futuras alterações nos marcos publicados pela ANVISA, com vistas à segurança do paciente e a manutenção das condições de segurança e eficácia dos produtos.

Roberto Latini