DECLARAÇÃO DE AUTORIDADE E COMPROMISSO DE CONFIDENCIALIDADE DA ADMINISTRAÇÃO DE ALIMENTOS E MEDICAMENTOS DOS ESTADOS UNIDOS PARA NÃO DIVULGAR PUBLICAMENTE INFORMAÇÕES NÃO PÚBLICAS COMPARTILHADAS PELA AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA DO BRASIL

A Agência Nacional de Vigilância Sanitária do Brasil (ANVISA) está autorizada a divulgar informações não públicas à Administração de Alimentos e Medicamentos dos Estados Unidos (FDA), sobre medicamentos regulados pela ANVISA, incluindo atividades pré e pós-mercado, conforme apropriado, como parte de atividades cooperativas de aplicação da lei ou regulatórias.

A FDA está autorizada, nos termos do 21 C.F.R. § 20.89[1], a divulgar informações não públicas à ANVISA sobre medicamentos regulados pela FDA, incluindo atividades pré e pós-mercado, conforme apropriado, como parte de atividades cooperativas de aplicação da lei ou regulatórias. Além disso, a FDA está autorizada, nos termos da seção 708(c) do Ato Federal de Alimentos, Medicamentos e Cosméticos[2], a compartilhar com um governo estrangeiro, conforme considerar apropriado e sob circunstâncias limitadas, certos tipos de informações secretas comerciais.

O Comissário de Alimentos e Medicamentos certificou a ANVISA como tendo autoridade e capacidade demonstrada para proteger informações secretas comerciais contra divulgação. Portanto, a FDA pode fornecer à ANVISA certos tipos de informações secretas comerciais a critério da FDA e mediante solicitação da ANVISA, com base nas seguintes certificações.

A FDA entende que algumas das informações que recebe da ANVISA podem incluir informações não públicas isentas de divulgação pública, como informações confidenciais comerciais, informações secretas comerciais, informações de privacidade pessoal, informações de aplicação da lei, informações designadas de segurança nacional ou informações internas pré decisórias. A FDA entende que essas informações não públicas são compartilhadas em confiança e que é crucial que a FDA mantenha a confidencialidade das informações não públicas trocadas. A divulgação pública de informações não públicas trocadas pela FDA poderia prejudicar seriamente qualquer interação científica e regulatória futura entre a ANVISA e a FDA. A ANVISA informará a FDA sobre o status não público das informações no momento em que as informações forem compartilhadas.

Portanto, a FDA certifica que:

1. tem a autoridade para proteger contra a divulgação pública de tais informações não públicas fornecidas a ela em confiança[3] pela ANVISA;

2. não divulgará publicamente tais informações não públicas fornecidas pela ANVISA sem a autorização por escrito do proprietário das informações, a autorização por escrito

[1] Código de Regulamentos Federais dos Estados Unidos, Título 21, seção 20.89.
[2] Código de Regulamentos Federais dos Estados Unidos, Título 21, seção 379(c).
[3] FDA tem a autoridade para proteger informações não públicas sob diversas provisões estatutárias

do indivíduo que é objeto das informações de privacidade pessoal, ou uma declaração escrita da ANVISA informando que as informações não têm mais status não público;

3. informará prontamente a ANVISA sobre qualquer esforço feito por mandado judicial ou legislativo para obter informações não públicas trocadas nos termos desta Declaração de Autoridade e Compromisso de Confidencialidade. Se tal mandado judicial ou legislativo ordenar a divulgação de tais informações não públicas, a FDA tomará todas as medidas apropriadas para garantir que as informações sejam divulgadas de forma que as proteja contra a divulgação pública;

4. informará prontamente a ANVISA sobre qualquer mudança nas leis dos Estados Unidos da América, ou em quaisquer políticas ou procedimentos relevantes que afetem sua capacidade de cumprir os compromissos deste documento;

5. estabeleceu e manterá a conformidade com os atuais quadros de Gerenciamento de Riscos e Segurança Cibernética do Instituto Nacional de Padrões e Tecnologia (NIST) do governo federal dos Estados Unidos[4], que são diretrizes e padrões de segurança de tecnologia da informação que visam proteger sistemas de informação e informações sensíveis compartilhadas;

6. protegerá os sistemas de informação que contenham informações não públicas fornecidas pela ANVISA em conformidade com as diretrizes e padrões atuais do NIST para garantir confidencialidade e integridade. Confidencialidade significa prevenir acesso não autorizado e divulgação de informações não públicas, e integridade significa proteger contra modificação ou destruição inadequadas de informações. A integridade inclui garantir o não repúdio e autenticidade das informações com base nos termos de segurança encontrados nesta Declaração de Autoridade e Compromisso de Confidencialidade, incluindo meios para proteger informações não públicas;

7. destruirá informações não públicas fornecidas pela ANVISA, seja em formato eletrônico ou impresso, assim que as informações forem utilizadas e não forem mais necessárias para fins oficiais, em conformidade com os requisitos federais de retenção de registros;

8. restringirá o acesso às informações não públicas fornecidas pela ANVISA aos funcionários e oficiais da FDA que necessitam de acesso a tais informações para desempenhar suas funções oficiais, de acordo com os usos autorizados das informações não públicas, a menos que autorizado por escrito pela ANVISA. A FDA informará a todos esses funcionários e oficiais (1) da natureza não pública das informações; e (2) da obrigação de manter tais informações não públicas;

[4] O Instituto Nacional de Padrões e Tecnologia (NIST) de Gerenciamento de Riscos e Segurança Cibernética fornecem um processo que integra atividades de segurança, privacidade e gerenciamento de riscos de cadeia de suprimentos cibernética ao ciclo de vida do desenvolvimento do sistema e fornece orientações baseadas em padrões, diretrizes e práticas para organizações gerenciarem e reduzirem os riscos de segurança cibernética, respectivamente. Essas estruturas de trabalho são principalmente destinadas a gerenciar e mitigar os riscos de segurança cibernética para organizações de infraestrutura crítica com base em padrões, diretrizes e práticas.

9. em caso de suspeita ou confirmação de incidente ou violação[5], incluindo um incidente de segurança cibernética[6] ou qualquer outro tipo de violação, seja intencional ou inadvertida:

(a) protegerá todas as informações não públicas fornecidas pela ANVISA, incluindo qualquer informação não pública criada, armazenada ou transmitida para evitar um incidente secundário de informações;

(b) relatará todos os incidentes ou violações suspeitos e confirmados envolvendo informações não públicas fornecidas pela ANVISA em qualquer meio ou formato, incluindo papel, oral ou eletrônico, à ANVISA o mais rápido possível e sem demora injustificada, no prazo máximo de um (1) dia após a descoberta ou detecção;

(c) fornecerá à ANVISA avaliações de impacto e gravidade de incidentes ou violações, após a ocorrência, incluindo uma descrição das medidas adotadas, incluindo medidas de segurança preventivas empregadas para lidar e remediar o incidente.

Este texto não tem a intenção de criar direitos e obrigações sob leis internacionais ou de outro tipo.

Assinado em nome da Administração de Alimentos e Medicamentos dos Estados Unidos.

_____/s/_____ ____9/30/24_____

Robert M. Califf, MD Data

Commissioner of Food and Drugs

U.S. Food and Drug Administration

10903 New Hampshire Avenue,

Silver Spring, Maryland

United States

[5] Um incidente é definido como "um evento que (1) efetiva ou iminentemente coloca em risco, sem autoridade legal, a confidencialidade de informações ou de um sistema de informação; ou (2) constitui uma violação ou ameaça iminente de violação da lei, políticas de segurança, procedimentos de segurança ou políticas de uso aceitável". Incidentes podem ser eventos envolvendo ameaças de segurança cibernética e de privacidade, como vírus, atividade maliciosa do usuário, perda de confidencialidade ou integridade, divulgação não autorizada ou destruição de informações. Para os fins deste acordo, violação é definida como um comprometimento real da segurança que resulta na divulgação não autorizada, perda, destruição acidental ou ilegal, alteração ou acesso a dados protegidos transmitidos, armazenados ou de outra forma processados. As violações podem ser intencionais ou inadvertidas.

[6] A segurança cibernética é a prevenção de danos a, proteção de, e restauração de computadores, sistemas de comunicações eletrônicas, serviços de comunicações eletrônicas, comunicação por fio e comunicação eletrônica, incluindo informações neles contidas, para garantir sua disponibilidade, integridade, autenticação, confidencialidade e não repúdio.