STATEMENT OF AUTHORITY
AND
CONFIDENTIALITY COMMITMENT FROM
AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA OF BRAZIL
NOT TO PUBLICLY DISCLOSE NON-PUBLIC INFORMATION SHARED
BY
THE UNITED STATES FOOD AND DRUG ADMINISTRATION

The United States Food and Drug Administration (FDA) is authorized under 21 C.F.R. § 20.89[1] to disclose non-public information to Agência Nacional de Vigilância Sanitária of Brazil (ANVISA) regarding FDA-regulated drugs, including pre- and post-market activities, as appropriate, as part of cooperative law enforcement or cooperative regulatory activities. FDA is further authorized under section 708(c) of the Federal Food, Drug, and Cosmetic Act[2] to share with a foreign government, as it deems appropriate and under limited circumstances, certain types of trade secret information.

The Commissioner of Food and Drugs has certified ANVISA as having the authority and demonstrated ability to protect trade secret information from disclosure. FDA therefore may provide ANVISA with certain types of trade secret information at FDA's discretion and upon request by ANVISA, based on the following certifications.

ANVISA understands that some of the information it receives from FDA may include non-public information exempt from public disclosure, such as commercially confidential information; trade secret information; personal privacy information; law enforcement information; designated national security information; or internal, pre-decisional information. ANVISA understands that this non-public information is shared in confidence and that it is critical that ANVISA maintains the confidentiality of exchanged non-public information. Public disclosure of exchanged non-public information by ANVISA could seriously jeopardize any further scientific and regulatory interactions between ANVISA and FDA. FDA will advise ANVISA of the non-public status of the information at the time that the information is shared.

Therefore, ANVISA certifies that it:

1. has the authority to protect from public disclosure such non-public information provided to it in confidence by FDA;

2. will not publicly disclose such FDA-provided non-public information without the written authorization of the owner of the information, the written authorization from the individual who is the subject of the personal privacy information, or a written statement from FDA providing that the information no longer has non-public status;

3. will protect trade secret information that FDA may provide from disclosure unless and until ANVISA is in possession of a written permission for disclosure by the sponsor of

---

[1] United States Code of Federal Regulations, Title 21, section 20.89.
[2] United States Code, Title 21, section 379(c).

the information provided by FDA, or alternatively of a declaration from the Commissioner of Food and Drugs of a public health emergency under section 319 of the Public Health Service Act that is relevant to the information;

4. with respect to trade secret information concerning the inspection of a drug facility, has the authority to otherwise obtain such information and will use such FDA-provided information only for civil, administrative regulatory purposes in the context of its mission;

5. will inform FDA promptly of any effort made by judicial or legislative mandate to obtain FDA-provided non-public information from ANVISA. If such judicial or legislative mandate requires disclosure of FDA-provided non-public information, ANVISA will take all appropriate legal measures in an effort to ensure that the information will be disclosed in a manner that protects the information from public disclosure;

6. will promptly inform FDA of any changes to the Brazil's laws, or to any relevant policies or procedures, that would affect ANVISA's ability to honor the commitments in this document;

7. has established and will maintain compliance with standards consistent with current United States federal government National Institute of Standards and Technology (NIST) Risk Management and Cybersecurity Frameworks[3] and/or International Organization for Standardization and International Electrotechnical Commission (ISO/IEC)[4] Information Technology security guidelines and standards that focus on protecting information systems and shared sensitive information;

8. will safeguard information systems that contain FDA-provided non-public information consistent with current NIST and/or ISO/IEC guidelines and standards to ensure confidentiality and integrity. Confidentiality means preventing unauthorized access to and disclosure of non-public information, and integrity means guarding against improper information modification or destruction. Integrity includes ensuring information non-repudiation and authenticity based on the security terms found in this Statement of Authority and Confidentiality Commitment, including means for protecting non-public information;

9. will destroy FDA-provided non-public information, whether in electronic form or hard copy form, once the information has been utilized and is no longer needed for official purposes in accordance with federal records retention requirements;

---

[3] The National Institute of Standards and Technology (NIST) Risk Management and Cybersecurity Frameworks provide a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle and provides guidance based on standards, guidelines, and practices for organizations to manage and reduce cybersecurity risk, respectively. These frameworks are primarily intended to manage and mitigate cybersecurity risk for critical infrastructure organizations based on standards, guidelines, and practices.

[4] The International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) is an international standard that assists organizations in managing the security of their information assets. It provides a management framework for implementing an information security management system to ensure the confidentiality of all corporate data. Foreign counterparts are strongly encouraged to meet the ISO 27001 standard requirements, or the most recent standard, and to be certified by an accredited certification body.

10. will restrict access to FDA-provided non-public information to the employees, and officials of ANVISA who require access to such non-public information to perform their official duties in accordance with authorized uses of the non-public information unless otherwise authorized in writing by FDA. ANVISA will advise all such employees and officials (1) of the non-public nature of the information; and (2) the obligation to keep such information non-public; and

11. will, in the event of a suspected or confirmed incident or breach[5], including a cybersecurity[6] incident, or any other type of breach, whether it is intentional or inadvertent:

(a) protect all FDA-provided non-public information, including any non-public information created, stored, or transmitted to avoid a secondary information incident;

(b) report all suspected and confirmed incidents or breaches involving FDA-provided non-public information in any medium or form, including paper, oral, or electronic, to FDA as soon as possible and without unreasonable delay, no later than one (1) day of discovery or detection; and

(c) provide to FDA impact and severity assessments of incidents or breaches, upon occurrence, including a description of the actions taken, including preventative security measures employed to address and remediate the incident.

This text is not intended to create rights and obligations under international or other law.

Signed on behalf of ANVISA:

ANTONIO BARRA TORRES
Director-President
Brazilian Health Regulatory Agency - ANVISA
Address: SIA5, AE 57, 71205-050. Brasília/DF. Brazil.

September 30 '24
Date

[5] An incident is defined as "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the confidentiality of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." Incidents can be events involving cybersecurity and privacy threats, such as viruses, malicious user activity, loss of confidentiality or integrity, unauthorized disclosure or destruction of information. For the purposes of this agreement, breach is defined as an actual compromise of security that results in the unauthorized disclosure of, loss, accidental or unlawful destruction, alteration, or access to protected data transmitted, stored, or otherwise processed. Breaches can be intentional or inadvertent.

[6] Cybersecurity is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

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

A Administração de Alimentos e Medicamentos dos Estados Unidos (FDA) está autorizada conforme 21 C.F.R. § 20.89[1] a divulgar informações não públicas à Agência Nacional de Vigilância Sanitária do Brasil (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. A FDA está ainda 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 em circunstâncias limitadas, certos tipos de informações secretas comerciais.

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

A ANVISA entende que algumas das informações que recebe da FDA podem incluir informações não públicas isentas de divulgação pública, como informações comercialmente confidenciais; informações secretas comerciais; informações de privacidade pessoal; informações de aplicação da lei; informações designadas de segurança nacional; ou informações internas e pré-decisórias. A ANVISA compreende que estas informações não públicas são compartilhadas em confiança e é fundamental que a ANVISA mantenha a confidencialidade das informações não públicas trocadas. A divulgação pública das informações não públicas trocadas pela ANVISA poderia comprometer seriamente quaisquer futuras interações científicas e regulatórias entre a ANVISA e a FDA. A FDA informará a ANVISA do status não público das informações no momento em que as informações forem compartilhadas.

Portanto, a ANVISA certifica que:

1. tem a autoridade para proteger contra divulgação pública tais informações não públicas fornecidas a ela em confiança pela FDA;
2. não divulgará publicamente tais informações não públicas fornecidas pela FDA sem a autorização por escrito do proprietário das informações, a autorização por escrito do indivíduo que é objeto das informações de privacidade pessoal, ou uma declaração por escrito da FDA informando que as informações não têm mais status não público;
3. protegerá as informações secretas comerciais que a FDA possa fornecer contra divulgação até que a ANVISA possua uma permissão por escrito para divulgação pelo

---

[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).

patrocinador das informações fornecidas pela FDA, ou alternativamente uma declaração do Comissário de Alimentos e Medicamentos de uma emergência de saúde pública nos termos da seção 319 do Ato de Serviço de Saúde Pública que seja relevante para as informações;

4. com relação às informações secretas comerciais referentes à inspeção de uma instalação de medicamentos, tem a autoridade para obter tais informações de outra forma e utilizar tais informações fornecidas pela FDA apenas para fins regulatórios civis, administrativos, no contexto de sua missão;
5. informará prontamente à FDA sobre qualquer esforço feito por mandado judicial ou legislativo para obter informações não públicas fornecidas pela FDA à ANVISA. Se tal mandado judicial ou legislativo exigir a divulgação de informações não públicas fornecidas pela FDA, a ANVISA tomará todas as medidas legais apropriadas para garantir que as informações sejam divulgadas de forma que as proteja contra a divulgação pública;
6. informará prontamente à FDA qualquer alteração nas leis do Brasil, ou em quaisquer políticas ou procedimentos relevantes, que possam afetar a capacidade da ANVISA de cumprir os compromissos deste documento;
7. estabeleceu e manterá a conformidade com padrões consistentes 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[3] e/ou diretrizes e padrões de segurança de tecnologia da informação da Organização Internacional de Normatização e Comissão Eletrotécnica Internacional (ISO/IEC)[4] que se concentram na proteção de sistemas de informação e informações sensíveis compartilhadas;
8. protegerá os sistemas de informação que contenham informações não públicas fornecidas pela FDA conforme os atuais padrões NIST e/ou ISO/IEC 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. Integridade inclui garantir a 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;
9. destruirá informações não públicas fornecidas pela FDA, seja em formato eletrônico ou impresso, assim que as informações forem utilizadas e não forem mais necessárias

---

[3] 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.

[4] A Organização Internacional de Normatização e Comissão Eletrotécnica Internacional (ISO/IEC) é um padrão internacional que ajuda as organizações a gerenciarem a segurança de seus ativos de informação. Ela fornece uma estrutura de trabalho gerencial para implementar um sistema de gerenciamento de segurança da informação para garantir a confidencialidade de todos os dados corporativos. É fortemente encorajado que os parceiros estrangeiros atendam aos requisitos do padrão ISO 27001, ou ao padrão mais recente, e sejam certificados por um organismo de certificação credenciado.

para fins oficiais, em conformidade com os requisitos federais de retenção de registros;

10. restringirá o acesso a informações não públicas fornecidas pela FDA aos funcionários e oficiais da ANVISA que necessitam de acesso a tais informações não públicas para realizar suas funções oficiais de acordo com os usos autorizados das informações não públicas, a menos que autorizado por escrito pela FDA. A ANVISA informará a todos esses funcionários e oficiais (1) da natureza não pública das informações; e (2) da obrigação de manter tais informações não públicas; e
11. em caso de incidente ou violação suspeita ou confirmada[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 FDA, incluindo quaisquer informações não públicas criadas, armazenadas ou transmitidas para evitar um incidente secundário de informação;

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

    (c) fornecerá à FDA avaliações de impacto e gravidade de incidentes ou violações, após sua ocorrência, incluindo uma descrição das ações tomadas, 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 ANVISA

30. Septembro '24

ANTONIO BARRA TORRES
Diretor-Presidente
Agência Nacional de Vigilância Sanitária – ANVISA
Endereço: SIA5, AE 57, 71205-050. Brasília/DF. Brasil.

Data

[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.