

**STATEMENT OF AUTHORITY
AND
CONFIDENTIALITY COMMITMENT FROM
THE UNITED STATES FOOD AND DRUG ADMINISTRATION
NOT TO PUBLICLY DISCLOSE NON-PUBLIC INFORMATION SHARED
BY
THE PHARMACEUTICAL SAFETY BUREAU, MINISTRY OF HEALTH, LABOUR,
AND WELFARE
AND
THE PHARMACEUTICALS AND MEDICAL DEVICES AGENCY OF JAPAN**

The Pharmaceutical Safety Bureau (PSB), Ministry of Health, Labour, and Welfare (MHLW) and the Pharmaceuticals and Medical Devices Agency (PMDA) of Japan are authorized to disclose non-public information to the United States Food and Drug Administration (FDA) regarding PSB and/or PMDA-regulated drugs, including pre- and post-market activities, as appropriate, as part of cooperative law enforcement or cooperative regulatory activities.

FDA is authorized under 21 C.F.R. § 20.89¹ to disclose non-public information to PSB and PMDA 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 Act² 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 PSB and PMDA as having the authority and demonstrated ability to protect trade secret information from disclosure. FDA therefore may provide PSB and PMDA with certain types of trade secret information at FDA's discretion and upon request by PSB and PMDA, based on the following certifications.

FDA understands that some of the information it receives from PSB and PMDA 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. FDA understands that this non-public information is shared in confidence and that it is critical that FDA maintains the confidentiality of exchanged non-public information. Public disclosure of exchanged non-public information by FDA could seriously jeopardize any further scientific and regulatory interactions between PSB and PMDA and FDA. PSB and PMDA will advise FDA of the non-public status of the information at the time that the information is shared.

¹ United States Code of Federal Regulations, Title 21, section 20.89.

² United States Code, Title 21, section 379(c).

Therefore, FDA certifies that it:

1. has the authority to protect from public disclosure such non-public information provided to it in confidence³;
2. will not publicly disclose such 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 PSB and PMDA providing that the information no longer has non-public status;
3. will promptly inform PSB and PMDA of any effort made by judicial or legislative mandate to obtain non-public information exchanged under the terms of this Statement of Authority and Confidentiality Commitment. If such judicial or legislative mandate orders disclosure of such non-public information, FDA will take all appropriate measures in an effort to ensure that the information will be disclosed in a manner that protects the information from public disclosure;
4. will promptly inform PSB and PMDA of any changes to the United States of America's laws, or to any relevant policies or procedures, that would affect its ability to honor the commitments in this document;
5. has established and will maintain compliance with current United States federal government National Institute of Standards and Technology (NIST) Risk Management and Cybersecurity Frameworks⁴ which are Information Technology security guidelines and standards that focus on protecting information systems and shared sensitive information;
6. will safeguard information systems that contain PSB and PMDA-provided non-public information in compliance with current NIST 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;
7. will destroy PSB and PMDA-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 line with federal records retention requirements;
8. will restrict access to PSB and PMDA-provided non-public information to the employees, and officials of FDA who require access to such non-public information to perform their official duties in line with authorized uses of the non-public information unless otherwise authorized in writing by PSB and PMDA. FDA will advise all such employees and officials of (1) the non-public nature of the information; and (2) the obligation to keep such information non-public; and

³ FDA has the authority to protect non-public information under several statutory provisions, including 5 U.S.C. § 552a; 5 U.S.C. § 552(b)(1) – (9); 18 U.S.C. § 1905; and 21 U.S.C. § 331(j).

⁴ 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.

9. will, in the event of a suspected or confirmed incident or breach⁵, including a cybersecurity⁶ incident, or any other type of breach, whether it is intentional or inadvertent,

- (a) protect all PSB and PMDA-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 PSB and PMDA-provided non-public information in any medium or form, including paper, oral, or electronic, to PSB and PMDA as soon as possible and without unreasonable delay, no later than one (1) day of discovery or detection; and
- (c) provide to PSB and PMDA 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 the domestic laws of either Japan or the United States or under international law.

Signed on behalf of the
United States Food and Drug Administration:

_____-/s/-_____
Mark Abdoo
Associate Commissioner
for Global Policy and Strategy

July 23, 2026
Date

U.S. Food and Drug Administration
10903 New Hampshire Avenue,
Silver Spring, Maryland
United States

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