



**STATEMENT OF AUTHORITY AND
CONFIDENTIALITY COMMITMENT FROM
THE HEALTH PRODUCTS AND FOOD BRANCH AND THE REGULATORY
OPERATIONS AND ENFORCEMENT BRANCH OF THE DEPARTMENT OF
HEALTH OF CANADA 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. § 20.89¹ to disclose non-public information to the Health Products and Food Branch (HPFB) and the Regulatory Operations and Enforcement Branch (ROEB) of the Department of Health of Canada (hereafter referred to as “HPFB and ROEB”), regarding FDA-regulated drugs, including pre- and post-market activities, as appropriate, as part of cooperative regulatory activities or law enforcement. 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.

This Statement of Authority and Confidentiality Commitment partially replaces two previously signed Confidentiality Commitments with respect to FDA-regulated drugs: the *Confidentiality Commitment Statement of Legal Authority and Commitment from Health Canada Not to Publicly Disclose Non-Public Information Shared by the U.S. Food and Drug Administration (USFDA), U.S. Department of Health and Human Services* signed on November 18, 2003, and the *Statement of Authority and Confidentiality Commitment From the Regulatory Operations and Regions Branch of the Department of Health of Canada Not to Publicly Disclose Non-Public Information Shared by the United States Food and Drug Administration* signed on February 26, 2018³. The above-mentioned Confidentiality Commitments from 2003 and 2018 will remain in effect for all other non-public information exchanged relating to FDA-regulated products that are not FDA-regulated drugs.

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

HPFB and ROEB understand that some of the information they receive 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. HPFB and ROEB understand that this non-public information is shared in confidence and that it is critical that HPFB and ROEB maintain the confidentiality

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

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

³ The Regulatory Operations and Regions Branch of the Department of Health of Canada was renamed to the Regulatory Operations and Enforcement Branch (ROEB) of Health Canada on January 30, 2019.



of exchanged non-public information. Public disclosure of exchanged non-public information by HPFB and ROEB could seriously jeopardize any further scientific and regulatory interactions between HPFB and ROEB and FDA. FDA will advise HPFB and ROEB of the non-public status of the information at the time that the information is shared.

Therefore, HPFB and ROEB certify that they:

1. have the authority to protect from public disclosure such non-public information provided to HPFB and ROEB in confidence by FDA;
2. will not publicly disclose such FDA-provided non-public information including trade secrets, 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 HPFB and ROEB is in possession of a written permission for disclosure by the sponsor of 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 mandate;
5. will inform FDA promptly of any effort made by judicial or legislative mandate to obtain FDA-provided non-public information, including trade secret information, exchanged under the terms of this Statement of Authority and Confidentiality Commitment. If such judicial or legislative mandate requires disclosure of such non-public information, HPFB and ROEB 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 Canada's laws, or to any relevant policies or procedures, that would affect HPFB's and ROEB'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 Frameworks⁴ and/or International Organization for Standardization and International Electrotechnical Commission (ISO/IEC)⁵ Information

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.

⁵ 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



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 promote 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 HPFB and ROEB records retention requirements;

10. will restrict access to FDA-provided non-public information to the employees, and officials of HPFB and ROEB 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. HPFB and ROEB 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 breach⁶, including a cybersecurity⁷ incident, or any other type of breach, whether it is intentional or inadvertent:

- (a) endeavour to 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) business day of discovery or detection; and

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.

⁶ 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.

⁷ 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.



- (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 the Health Products and Food Branch (HPFB) and the Regulatory Operations and Enforcement Branch (ROEB) of the Department of Health of Canada

_____/s/_____
Pamela Aung-Thin
Assistant Deputy Minister
Health Products and Food Branch

01/09/2025
Date

Health Canada
Health Products and Food Branch
Main Building
150 Tunney's Pasture Driveway,
Ottawa, Ontario
Canada

_____/s/_____
Linsey Hollett
Assistant Deputy Minister
Regulatory Operations and Enforcement Branch

01/08/2025
Date

Health Canada
Regulatory Operations and Enforcement Branch
Jeanne Mance Building
200 Eglantine Driveway, Tunney's Pasture,
Ottawa, Ontario
Canada