SMG 2830.4

FDA Staff Manual Guides, Volume III – General Administration

Agreements with Other Government Agencies – International Arrangements with Foreign Government Agencies and International Organizations

Confidentiality Commitments; Responding to Unauthorized Disclosure of Non-Public Information

Effective Date: 01/04/2023
Changed: 01/12/2023

1. Purpose

This Staff Manual Guide (SMG) establishes general, FDA-wide policies and procedures for responding to incidents of unauthorized disclosure of non-public information (NPI) exchanged between FDA and Foreign Government Agencies or

International Organizations, hereafter referred to as foreign counterparts. This document applies whether the unauthorized disclosure is done by FDA or the foreign counterpart. The policies in this SMG apply whether it is FDA or the foreign counterpart's NPI that has been disclosed in an unauthorized manner.

The purpose of this FDA-wide SMG is to ensure consistency across FDA Components in identifying unauthorized disclosures of NPI; responding to disclosure incidents; and understanding the roles and responsibilities of FDA Components in responding to incidents of unauthorized disclosure.

FDA Components may also have specific written procedures for handling unauthorized disclosure incidents.

The provisions of this document should be implemented to notify affected parties and address unauthorized disclosures of FDA or a foreign counterpart's NPI.

2. Background

FDA fosters international partnerships with Foreign Government Agencies and International Organizations (also referred to as foreign counterparts). As part of these partnerships, FDA may have a need to share and receive NPI in certain situations, such as during an outbreak investigation, or to alert a Foreign Government Agency to violative inspectional findings at a firm, or for routine information sharing. All sharing of NPI must be pursuant to a signed Confidentiality Commitment from the foreign counterpart and/or other appropriate written authorizations, as needed.

FDA relies on Confidentiality Commitments to memorialize agreements with foreign counterparts to protect shared NPI from disclosure. Confidentiality Commitments describe the requirements for sharing of NPI under applicable laws, as well as any other terms or conditions negotiated by FDA and the foreign counterpart. When the FDA or the foreign counterpart discloses NPI in a manner that is inconsistent with the Confidentiality Commitment, there are potential legal consequences. The owner of disclosed NPI may pursue civil remedies, including monetary damages, against FDA and agency staff if NPI is improperly disclosed. Also, FDA employees may be subject to criminal penalties under the Federal Food, Drug, and Cosmetic Act, the Trade Secrets Act, or other applicable law, if NPI is improperly disclosed.

When FDA staff plan to share NPI with a foreign counterpart, or when they receive NPI in reliance on a Confidentiality Commitment, they should do so following all applicable policies and procedures, including adhering to SMG 2830.3, "Sharing Non-Public Information with Foreign Government Officials" and by working with the appropriate FDA Component.

All FDA staff should follow the procedures outlined in this SMG, as well as adhere to any other specific written procedures provided by their FDA Component, when

responding to unauthorized disclosures of NPI. FDA staff should act quickly to address incidents of unauthorized disclosure.

3. Policy

This SMG describes the FDA-wide procedures for responding to unauthorized disclosure of NPI exchanged between FDA and foreign counterparts in reliance on Confidentiality Commitments. It also reflects FDA's policy decisions governing the sharing of NPI as described in Staff Manual Guide (SMG) 2830.3, "Sharing Non-Public Information with Foreign Government Officials". All FDA staff, including those who are authorized to share NPI with foreign counterparts, should adhere to the procedures set forth in this SMG, as well as to any other specific written procedures provided by their FDA Component or that apply to all Components, when responding to unauthorized disclosures of NPI.

4. Scope

This procedure applies to all FDA Components, including FDA Headquarters and Foreign Office staff, responding to unauthorized disclosures of NPI shared in reliance on a Confidentiality Commitment. This procedure applies to unauthorized disclosures of FDA's NPI provided to foreign counterparts and the unauthorized disclosure of a foreign counterpart's NPI provided to FDA. Unauthorized disclosures may be intentional or inadvertent and can be made by a Confidentiality Commitment participant or be the result of a breach of information through a security incident impacting a foreign counterpart or FDA's systems. Refer to SMG 2830.3 for more information on Agency-wide policies and procedures for the proper sharing and receiving of NPI with foreign counterparts.

5. Definitions

A. Definitions Concerning Disclosure of Non-Public Information

- **Non-Public Information (NPI)** -- Information that is protected from disclosure to the public by U.S. law, such as the Freedom of Information Act, the Privacy Act, or the Trade Secrets Act. Examples of NPI include confidential commercial information, trade secret information, pre-decisional FDA communications or documents (such as draft regulations or draft guidance documents), and personal privacy information. Information that FDA would not disclose under 21 CFR Parts 20 or 21 or is legally prohibited from disclosure under Parts 20 or 21 or applicable statute is considered NPI. NPI

may be information owned by a party outside FDA or internal FDA information.

- **Unauthorized Disclosure of NPI** -- Any disclosure of NPI that violates the commitments established in the applicable Confidentiality Commitment or deviates from the Staff Manual Guide 2830.3 or applicable law. Unauthorized disclosure includes sharing NPI with anyone in an agency that is not identified as a participant in the Confidentiality Commitment and therefore is not bound by the Confidentiality Commitment. Unauthorized disclosures can take place over the phone, e-mail, web conferencing and collaboration platforms, in person, any other mode of information transmission, or by a breach of information through a cybersecurity incident. Disclosure of NPI that violate a Confidentiality Commitment includes disclosures without the consent of the owner or sponsor and disclosures without a statement from the providing foreign counterpart that the NPI is no longer non-public. Unauthorized disclosures may be intentional or inadvertent. Unauthorized disclosures can take place with any unauthorized third party, including:
    - another Foreign Government Agency;
    - another International Organization;
    - another U.S. government agency;
    - any branch or unit of a Foreign Government Agency or International Organization who has not provided FDA with a Confidentiality Commitment;
    - any person; or
    - any physical or systems-related information breach, including cybersecurity incidents when FDA's NPI or a foreign counterpart's NPI is unlawfully accessed.

B. Definitions Concerning FDA Terms

- **Confidentiality Commitment (CC)** – A document that a foreign counterpart concludes with FDA pursuant to 21 C.F.R. § 20.89 or section 708(c) of the Federal Food, Drug, and Cosmetic Act that contains, among other provisions, a written statement establishing FDA or the foreign counterpart's authority to protect NPI from public disclosure and a written commitment not to disclose any such information provided by FDA or the foreign counterpart without the written permission of the owner or sponsor or written confirmation by the source agency/organization that the information no longer has confidential status.

- **FDA Components (also referred to as FDA Centers and Offices) - with the aid of its Freedom of Information (FOI)/Disclosure Office and the**

Component International Office – Generally responsible for managing foreign counterpart requests for FDA's NPI and managing NPI received from foreign counterparts. Component management responsibilities include handling requests for NPI; deciding whether to share the information; when applicable, obtaining consent from sponsor or owner of the information; making proper redactions; ensuring the appropriate FDA official has authorized the sharing and transmitting of information; and handling NPI received from foreign counterparts. See SMG 2830.3 for more information.

- **Office of Global Policy and Strategy (OGPS), Office of Trade and Global Partnerships (OTGP) –** Serves as the FDA lead for addressing and coordinating issues involving the development or implementation of Confidentiality Commitments. OTGP also serves as a resource for FDA Components during Component responses to unauthorized disclosure incidents and maintains records of disclosure incidents. In the event of an unauthorized disclosure made by a foreign counterpart where the NPI of multiple Components has been impacted, OTGP will work with the Components to coordinate FDA's response.

- **OGPS Foreign Office** – The OGPS Office (whether at headquarters or abroad) handling the portfolio that includes responsibility for interactions with and analyses of the relevant foreign counterparts within a particular country or region.

  NOTE: When OGPS Foreign Offices plan to share NPI with foreign counterparts or receive NPI from foreign counterparts, the Foreign Offices should work with the relevant Component who has jurisdiction over the product whose NPI will be discussed to ensure adherence with the proper policies and procedures for sharing and receiving NPI.

- **Office of the Commissioner, Office of the Chief Counsel (OCC)** – Provides legal review, and assesses issues related to unauthorized disclosures, when necessary, to minimize legal risks. OCC advises Components on legal matters and represents FDA in administrative hearings and certain court proceedings.

- **Office of Regulatory Affairs (ORA), Office of Criminal Investigations (OCI), Office of Internal Affairs (OIA)** – OCI has the primary responsibility for criminal investigations conducted by the FDA and for all law enforcement and intelligence issues pertaining to threats against FDA-regulated products and entities. OCI-OIA is responsible for obtaining information for the FDA on any matter relating to allegations of misconduct, impropriety, conflict of

interest, or other violations of Federal statutes by FDA staff, including unauthorized disclosure of NPI.

- **Office of the Commissioner, Office of Digital Transformation, Office of Information Security (OIS)** – The Office of Information Security, led by the Chief Information Security Officer (CISO), directs and implements the FDA Cybersecurity, Counterintelligence, and Insider Threat Program to ensure security controls are appropriately applied to FDA systems for the protection of privacy and to ensure the confidentiality, integrity, and availability of information. The CISO enforces cybersecurity standards and security control parameters that comply with the Office of Management and Budget (OMB), Federal Information Security Modernization Act (FISMA), the Federal Risk and Authorization Management Program (FedRAMP), HHS, and other federal government security requirements.
- **FDA Privacy Program –** The Privacy Program administers FDA's privacy compliance, Privacy Act, and breach response (reported incidents involving personally identifiable information (PII)) activities. The Privacy Act Officer and staff are responsible for conducting and coordinating agency actions addressing reported breaches.

C. Definitions Concerning the Foreign Government Agency or International Organization

- **Foreign Counterpart** – A Foreign Government Agency or International Organization with similar regulatory authorities and functions to FDA, including, but not limited to, administrative or regulatory law enforcement, product application review, compliance review, standard-setting, regulatory research, policy development, development and drafting of laws and regulations, and post market surveillance. For this SMG, both Foreign Government Agencies and International Organizations with whom FDA has a Confidentiality Commitment are considered foreign counterparts.
- **Foreign Government Agency** – A unit of a foreign government that may have regulatory authorities similar to FDA. Under certain circumstances, supranational entities (e.g., the European Medicines Agency (EMA) or some other institutions of the European Union) or subnational entities (e.g., provinces or states within a foreign country) with appropriate responsibilities may be considered Foreign Government Agencies for the purposes of this SMG.
- **International Organization** – An organization established by law, treaty, or other governmental action and having the responsibility to facilitate global or regional harmonization of standards and requirements in FDA's areas of responsibility or to promote and coordinate public health efforts. International groups that do not meet this definition are not eligible to sign a Confidentiality Commitment and receive NPI under 21 C.F.R. § 20.89. Examples of entities

considered International Organizations for purposes of this SMG include, but are not limited to, the World Health Organization (WHO), the Pan American Health Organization (PAHO) and other regional offices of the WHO, and the Food and Agricultural Organization (FAO) of the United Nations.

6. Responsibilities and Procedure

FDA Component staff must address unauthorized disclosures of NPI immediately. In all cases, responses should consist of a series of measures designed to prevent further disclosure of the NPI, protect the interests of the owner of the information, reverse or mitigate the disclosure where possible, and ensure similar disclosures do not recur in the future. Responses to unauthorized disclosures of NPI may depend on circumstances specific to the nature of the disclosure, including who made the disclosure, the category of NPI that is disclosed, and the type of breach that occurred (e.g., cybersecurity incident).

All FDA Components must adhere to the following procedures when responding to unauthorized disclosures of NPI.

A. General Process: Responding to Unauthorized Disclosure of FDA's Non-public Information by a Foreign Counterpart: for example, if the foreign counterpart shares FDA-provided NPI with another entity that is not covered by the Confidentiality Commitment; or if a foreign counterpart's information systems are breached through a cybersecurity or physical security incident, resulting in the unlawful access to FDA-provided NPI.

1. Immediate Action

a. After an initial review and assessment of the incident, the affected Component(s) should, in consultation with OGPS, determine whether further information sharing with the foreign counterpart should be halted until an extensive review of the incident is complete.

NOTE: Any FDA designee (see SMG 1410.65 and SMG 1410.66) can decide to stop information sharing. In the case of a breach impacting the NPI of multiple Components, or if there was a cybersecurity incident of a foreign counterpart's system, OGPS will consult with Component leadership, OCC, OCI-OIA, and OIS about additional immediate and longer-term response measures. In such cases, OGPS will work with Components to determine if information sharing should be halted and, if halted, whether and when sharing of NPI may resume.

b. If applicable, request the foreign counterpart inform the unauthorized recipient directly that received information is non-public and should not have been disclosed to them. Coordinate with the foreign counterpart to ensure that the recipient understands they are not authorized to use,

share, reproduce, or retain the received information in any way. Ask that the recipient destroy, delete, or return all originals and copies of the NPI, this includes requesting written confirmation that all the information has been destroyed or returned to the foreign counterpart. Hardcopy or electronic confirmation is acceptable.[1]

2. Reporting

As soon as possible, report the unauthorized disclosure to:

a. FDA Component International and Freedom of Information (FOI)/Disclosure offices.
b. OTGP at oc-ogps-ia@fda.hhs.gov and the OGPS Foreign Office, if applicable.
c. OTGP will notify OGPS Associate Commissioner. OTGP will also notify other FDA Components and OCC when the unauthorized disclosure of NPI impacts multiple Components, OCI-OIA at contact.oia@fda.hhs.gov if it is related to a law enforcement or intelligence matter, and OIS at CIOCC@fda.hhs.gov if it is related to a cybersecurity incident.

NOTE: Through Confidentiality Commitments, foreign counterparts have committed to reporting all suspected and confirmed incidents or breaches, including a cybersecurity incident, or any other type of breach, whether it is intentional or inadvertent, involving FDA-provided NPI 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. Foreign counterparts should provide to the FDA impact and severity assessments of incidents or breaches, upon occurrence, including a description of the actions taken and preventative security measures employed to address and remediate the incident.

3. Evaluate Information and Notify Owner

a. Work with the FDA Component International and FOI/Disclosure Offices to evaluate and identify the type of NPI impacted by the unauthorized disclosure (e.g., confidential commercial information; trade secret information; personal privacy information; law enforcement information, or internal, pre-decisional information). Identify the owner of the information in the case of breach of personal privacy information,

[1] Advice to destroy/delete information is not intended to supersede any legal requirement to retain records. If the recipient of the unauthorized disclosed information indicates that he/she is prohibited from destroying/deleting the information, the relevant FDA Center/Office disclosure staff should be contacted for additional guidance.

or company information (e.g., confidential commercial information or trade secret information).

1) If FDA pre-decisional information was impacted in the unauthorized disclosure, FDA Components should evaluate impact of breach and take any follow-up and/or mitigation steps necessary.
2) If personal privacy information was impacted in the unauthorized disclosure, contact FDA's Privacy Program at fdaprivacyoffice@fda.hhs.gov for further action. Do NOT ask the Foreign Counterpart to notify the subjects of the personal privacy information and do not attempt to notify any subjects directly prior to obtaining guidance from the Privacy Act Officer.
3) If confidential commercial information and/or trade secret information was impacted in the unauthorized disclosure, request the foreign counterpart notify the owner. In the communication to the information owner, the foreign counterpart should avoid identifying: (i) the employee who made the unauthorized disclosure; and (ii) the recipient(s) of the unauthorized disclosed information
4) If applicable, the foreign counterpart should notify FDA again once it has informed the information owner of the disclosure incident.

   NOTE: The foreign counterpart, or FDA, if applicable, should send written communications such that receipt can be confirmed. Hardcopy or electronic confirmation is acceptable. Communications sent electronically by FDA should be encrypted using FDA's Secure Email Program.

b. Consult OTGP, OCC, and OCI-OIA if the information owner requests any of the following information from the FDA:
   1) Additional information, such as the name of the recipient(s) of the unauthorized disclosed information;
   2) Name of the foreign counterpart employee responsible for the unauthorized disclosure; or
   3) Meeting or conference call to discuss the unauthorized disclosure.
c. Consult with OTGP and OCC to inquire whether additional steps are necessary to address or mitigate legal vulnerabilities, especially in cases where the recipient of the information refuses to return or destroy the information.

4. Follow-up Action with Foreign Counterpart

a. OTGP and affected Components should evaluate the cause of the unauthorized disclosure and determine whether mitigation measures should be taken to avoid similar disclosures in the future.

b. OTGP and OGPS leadership, in consultation with Components and OCC, will:

1) Assess if additional safeguards (e.g., IT safeguards, physical safeguards, training or re-training for staff, or other policy and procedural safeguards) should be added, or if modifications should be made to the information sharing process or the Confidentiality Commitment to prevent additional unauthorized disclosures by the foreign counterpart in the future. OGPS/OTGP may also propose terminating the Confidentiality Commitment if there are concerns about the foreign counterpart's ability to protect NPI.

2) Draft communication to the foreign counterpart with the following information as applicable: reminder of their commitment to protect FDA's information under the terms of the Confidentiality Commitment, request the foreign counterpart provide an explanation for mitigating similar incidents in the future, and request for any additional safeguards (see 4.b.(1) above).

NOTE: If not already provided by the foreign counterpart, the communication should include a request for impact and severity assessments of the incident(s) involving FDA-provided NPI, including a description of the actions and preventive security measures taken to address and remediate the incident(s).

3) Clear the draft communication to the foreign counterpart through the OGPS Associate Commissioner, OGPS Foreign Office, OCC, OIS and relevant FDA Components.

4) Send written communications to the foreign counterpart such that receipt can be confirmed.

NOTE: If information sharing with the foreign counterpart has been halted, the Component(s), in consultation with OGPS and OCC, should decide whether it should resume.

5. Recordkeeping

a. OTGP, with input from Components and Foreign Offices, should record all relevant information regarding the incident in the OTGP-managed incident tracker. To gain access to the tracker, contact OTGP at oc-ogps-ia@fda.hhs.gov.

b. OTGP will create and save a file that documents the actions taken in response to the unauthorized disclosure, including copies of all written communications sent by FDA.

B. General Process: Responding to Unauthorized Disclosures of Foreign Counterpart's Non-public Information by FDA: for example, if Component staff discloses foreign counterpart-provided NPI with another entity that is not covered by the Confidentiality Commitment; or if FDA's information systems are breached through a cybersecurity or physical security incident, resulting in the unlawful access to foreign counterpart-provided NPI.

1. Reporting

a. As soon as possible, report the unauthorized disclosure to:

1) FDA Component leadership, International and FOI/Disclosure offices.

2) OTGP at oc-ogps-ia@fda.hhs.gov and the OGPS Foreign Office, if applicable.

3) OTGP will notify OGPS Associate Commissioner along with notifying OCC and OCI-OIA at contact.oia@fda.hhs.gov if an FDA employee made the unauthorized disclosure or if it is related to a law enforcement or intelligence matter. In the event of a cyber security or physical security incident impacting the FDA and/or foreign counterpart-provided NPI, OTGP will notify OIS at CIOCC@fda.hhs.gov.

b. Notify the foreign counterpart of the unauthorized disclosure as soon as possible, within one (1) day of discovery or detection. If available, FDA should provide the foreign counterpart impact and severity assessments of the incident, including a description of the actions taken to address and remediate the incident.

c. Discuss next steps with the foreign counterpart, including notifying the unauthorized recipient(s) and providing additional information regarding the disclosure incident. In the communications to the foreign counterpart, identify the NPI impacted and additional details about the incident, but avoid identifying the employee who made the unauthorized disclosure. Identifying recipients of the unauthorized disclosed information is permitted under this SMG. Upon identifying the unauthorized recipients, FDA should have a general sense of what type of NPI was impacted, even if it has not completed its full evaluation.

2. Evaluate Information and Notify Unauthorized Recipient

a. Work with the FDA Component International and FOI/Disclosure Offices, and the FDA Privacy Act Officer to evaluate and identify the type of NPI impacted by the unauthorized disclosure (e.g., confidential

commercial information; trade secret information; personal privacy information; law enforcement information, or internal, pre-decisional information), and coordinate a response.

b. Notify the unauthorized recipient directly or through the foreign counterpart, where appropriate, that the information is non-public, and that they are not authorized to share or retain it. Request that the recipient provide written confirmation that the recipient has destroyed, deleted, or returned the NPI and any NPI copies.[2] If contact with recipient is by phone, notify recipient that the FDA Component staff will follow up by email. Outgoing FDA written communications about the unauthorized disclosure should be sent such that receipt can be confirmed. Components should work with their International and FOI/Disclosure staff to draft communications to unauthorized recipients.

c. Communicate with the foreign counterpart about actions taken by FDA and any progress made to remediate the incident. If necessary, develop follow-up written communications to the foreign counterpart with additional details of the unauthorized disclosure. If not already done so (see section B.1.c.), Components should provide the foreign counterpart with impact and severity assessments of incidents or breaches upon occurrence and a description of preventative security measures employed to address and remediate the incident.

d. Clear the draft communications to the foreign counterpart with OGPS, OCC, OCI-OIA, OIS, and FDA Components.

e. Send written communications to the foreign counterpart such that receipt can be confirmed.

NOTE: With unauthorized disclosure of foreign counterpart-provided NPI, FDA should request that the foreign counterpart contact all sponsors/companies impacted by the unauthorized disclosure. FDA is not required but may consider notifying the owner or subject of the information (e.g., sponsor or individual) if confidential commercial information, trade secret information or personal privacy information that was provided to FDA by a foreign counterpart was impacted.

f. Consult OTGP, OCC, and OCI-OIA if the foreign counterpart requests any of the following information:

[2] Advice to destroy/delete information is not intended to supersede any legal requirement to retain records. If the recipient of the unauthorized disclosed information indicates that he/she is prohibited from destroying/deleting the information, the relevant FDA Center/Office disclosure staff should be contacted for additional guidance.

1) Additional information about the unauthorized disclosed information;
2) Name of the FDA employee responsible for the unauthorized disclosure; or
3) Meetings or conference calls to discuss the unauthorized disclosure.

g. Consult with OTGP staff and OCC to inquire whether additional steps are necessary to address or mitigate legal vulnerabilities.

3. Internal FDA Follow-up Action

a. OTGP, OCC, OIS and affected Component(s) should evaluate and discuss the cause of the unauthorized disclosure and determine whether mitigation measures should be taken to avoid similar disclosures in the future, such as re-training of FDA staff, changes to processes for sharing information, or amending Confidentiality Commitments.

4. Recordkeeping

a. OTGP, with input from Components and Foreign Offices, will record all relevant information regarding the incident in the OTGP-managed incident tracker. To gain access to the tracker, contact OTGP at oc-ogps-ia@fda.hhs.gov.

b. OTGP will create and save a file that documents the actions taken in response to the unauthorized disclosure, including copies of all written communications sent by FDA.

7. References

A. 21 C.F.R. § 20.89, Communications with Foreign Government Officials
B. 21 U.S.C. § 379, Federal Food, Drug and Cosmetic Act
C. 21 U.S.C. § 301(j), Federal Food, Drug and Cosmetic Act
D. 18 U.S.C. § 1905, Trade Secrets Act
E. Staff Manual Guide 2830.3, Sharing Non-Public Information with Foreign Government Officials

8. Effective Date

The effective date of this guide is January 4, 2023.

9. Document History – SMG 2830.4, "Confidentiality Commitments; Responding to Unauthorized Disclosure of Non-Public Information"

Status (I, R, C)	Date Approved	Location of Change History	Contact	Approving Official
Initial	12/22/2022	N/A	OC/OGPS/ OTGP	Mark Abdoo, Associate Commissioner for Office of Global Policy and Strategy
Change	01/10/2023	Amend OTMRIA to OTGP	OC/OGPS/ OTGP	Joseph Rieras, Director, Office of Trade and Global Partnerships

ATTACHMENT A

Unauthorized Disclosure Response Checklist

This checklist serves as a resource to guide FDA Components through the process of addressing unauthorized disclosures of Non-Public Information (NPI). Completion of this checklist is not mandatory.

- ☐ Unauthorized disclosure occurred or was discovered. **Date**: _____
- ☐ Component notified Component International staff, Freedom of Information (FOI)/Disclosure office, and Office of Global Policy and Strategy (OGPS) Foreign Office (if applicable) of the unauthorized disclosure. **Date**:_____
- ☐ Component notified OGPS, Office of Trade and Global Partnerships (OTGP) **Date**:_____
- ☐ OTGP notified Office of Chief Counsel (OCC) *(if applicable)* **Date**:_____
- ☐ OTGP notified Office of Information Security (OIS) *(if applicable)* **Date**:_____
- ☐ OTGP notified ORA's Office of Criminal Investigations (OCI), Office of Internal Affairs (OIA) *(if applicable)* **Date:** _____
- ☐ FDA Component International and FOI/Disclosure staff evaluated and identified the type of NPI impacted by the unauthorized disclosure **Date**: _____
- ☐ Identified the owner of the information, in the case of breach of personal privacy information, or company information (e.g., confidential commercial information and/or trade secret information). **Date**: _____
- ☐ Unauthorized recipient(s) notified by phone or email **Date**: _____
    - ☐ Received written or verbal confirmation from recipient(s) regarding disposition of inadvertently disclosed information **Date**: _____
- ☐ Information owner notified via written notification. **Date**: _____
    - ☐ Received written confirmation of notification from information owner.

      Date: _____
- ☐ Evaluated the cause of the unauthorized disclosure and determined what steps can be taken, if any, to avoid similar unauthorized disclosures in the future (e.g., process changes, retraining). **Date**: _____
- ☐ OTGP recorded unauthorized disclosure in Unauthorized Disclosure Incident Tracker. **Date**: _____

ATTACHMENT B

Example Notification Letter to Sponsor/Information Owner[3]

DATE

Sponsor/Information Owner address

Dear [Sponsor/Information Owner]:

This letter is to inform you that the U.S. Food and Drug Administration (FDA) has been advised by the [foreign counterpart] that FDA information in [acronym for foreign counterpart]'s possession, namely an [type of information disclosed] pertaining to [Sponsor or information owner name], was [disclosed to an unauthorized recipient, unlawfully accessed, etc.].

On [date], FDA found that certain records containing, in whole or in part, non-public information including [trade secret information, confidential commercial information, and personal information] pertaining to [Sponsor name] was [disclosed to an unauthorized recipient, unlawfully accessed, etc.]. FDA had provided the record to [foreign counterpart] pursuant to a Confidentiality Commitment between the FDA and [foreign counterpart]. Specifically, the following record was unlawfully accessed: [insert description of records]. A copy of these records is enclosed. The attached version of these records was identified by [foreign counterpart] as having been unlawfully accessed.

[Acronym of foreign counterpart] has indicated that immediately after its detection of the incident, [acronym of foreign counterpart] took action to prevent further disclosure, including [description of foreign counterpart's response]. FDA understands that you may have concerns about what this means for your company. If you have any follow-up questions relating to the unauthorized disclosure, you may contact FDA [or in certain cases, the foreign counterpart].

[3] This letter serves as an example for notifying the information owner of an unauthorized disclosure and may be modified as needed to address specific incidents. For example, letter can state that Foreign Government Agency has provided FDA with a reassurance that the unintended recipient has agreed to destroy and not retain any copies, nor further disseminate the records. "Owner" does not necessarily include individual subjects of PII impacted by the disclosure.

ATTACHMENT B

FDA takes its disclosure responsibilities seriously, and we make every effort to ensure that information is disclosed only in accordance with applicable laws and regulations.

If you have any questions, please contact [FDA point of contact] at [point of contact's telephone number].

ATTACHMENT C

Example Notification Letter to Foreign Counterpart[4]

DATE

Foreign counterpart address

Dear [foreign counterpart]:

This letter is to inform you that the Food and Drug Administration (FDA) has found that non-public information in FDA's possession provided to it by [foreign counterpart], was [unlawfully accessed, disclosed to an unauthorized recipient, etc.].

On [date], FDA found that certain records containing, in whole or in part, non-public information including [trade secret information, confidential commercial information, and personal information] pertaining to [Sponsor name] was [unlawfully accessed, disclosed to an unauthorized recipient, etc.]. [foreign counterpart] had provided the record to FDA pursuant to a Confidentiality Commitment between the FDA and [acronym of foreign counterpart]. Specifically, the following record was impacted: [insert description of records]. A copy of these records is enclosed. The attached version of these records was identified by FDA as having been [unlawfully accessed, disclosed to an unauthorized recipient, etc.].

Immediately after its detection of the incident, FDA has taken the following actions to address the unauthorized disclosure of non-public information: [description of FDA's response].

FDA takes its disclosure responsibilities seriously, and we make every effort to ensure that information is disclosed only in accordance with applicable laws and regulations.

If you have any questions, please contact [FDA point of contact] at [FDA contact phone number].

[4] This letter serves as an example for notifying the Foreign Government Agency or International Organization of an unauthorized disclosure and may be modified as needed to address specific incidents.

ATTACHMENT D

Unauthorized Disclosure Incident Tracker

This attachment is a resource for FDA Components when submitting information for the Unauthorized Disclosure Tracker, managed by OTGP. To gain access to the tracker, contact OTGP at oc-ogps-ia@fda.hhs.gov.

Foreign Counterpart or FDA NPI	**Disclosure Description**	**Type of Disclosure**	**Counterpart Standing**	**Date Reported**	**Assigned to**	**FDA Response**	**Counterpart Response**	**Associated Files**	**Issue Logged by**
Which foreign counterpart or FDA Component's NPI is affected by the disclosure?	*How and when did the breach occur?* *Who was affected (including specific U.S. companies that may need to be contacted)?* *What information was disclosed?* *What type of NPI was involved?* .	*Choose the type of disclosure: intentional, inadvertent, cyber incident, other.*	*What is the counterpart's current information sharing standing with FDA?* *Positive (no previous issues),* *Previous Disclosures (previous experiences with unauthorized disclosures – either intentional or inadvertent),* *Not Sharing (FDA is currently not sharing NPI with the counterpart)*	*When was the breach reported to the FDA?*	*Who in the FDA is managing communications and actions regarding the breach?*	*What actions did FDA take in response to the breach?* *What formal communication was sent to the sponsor/owner of the information?*	*What actions has the foreign counterpart taken in response to the breach?*	*What files are pertinent to this breach?*	*Who is logging the issue into the tracker?*