Policy on the Protection of Personal Information

Novartis Global Policy

January 1, 2016

Version PPI 001.V2.EN

Version History

Dated	Author	Changes
1 January 2008	D. Fabian Masoch	Version 1.0
26 May 2015	K. Mager	Version 2.0

NOVARTIS

1. Introduction

1.1 Purpose

To support its mission of Caring and Curing, Novartis uses Personal Information in the development of new therapies, marketing of innovative products, partnering with health care professionals and researchers, and in relation to its Associates. Novartis respects the privacy rights of any person whose Personal Information we are entrusted with, and Novartis complies with laws and regulations protecting Personal Information.

This Policy explains the relevant data privacy principles for the protection of Personal Information and how such principles are to be implemented.

1.2 Scope and Applicability

This Policy covers all Personal Information collected, processed, shared, or used by Novartis.

It applies to all Associates*.

This Policy contains Novartis' global standards.

This Policy enters into force as of January 1, 2016 and must be implemented by all Novartis affiliates. It replaces the previous version of the Policy on the Protection of Personal Information dated January 1, 2008.

*Directors, officers, managers and employees of Novartis AG and its affiliates ("Novartis")

2. Principles and Rules

2.1 Compliance with Law

Principles and Rules

Novartis aspires to be a trusted healthcare partner and a good corporate citizen. Our Code of Conduct contains fundamental principles and rules concerning ethical business conduct, including the recognition of the privacy rights and commitment to the protection of Personal Information of our Associates and other persons whose Personal Information is shared with Novartis.

As Associates, we have a specific responsibility to respect this commitment, as described in this Policy and expressed in relevant data privacy laws.

Associates are expected to recognize if they are collecting, processing, sharing or using Personal Information. Associates must be aware of the general privacy requirements and principles that govern Personal Information and know when to escalate issues to their local Data Privacy Officer.

The Data Privacy program at Novartis provides guidance, training and knowledgeable individuals to assist you in understanding and meeting your obligations.

Definitions

"Personal Information" means all information that relates to a person where that person can be identified by you or others. In some cases, the person can be identified directly (e.g., your name or your photograph) or the person can be identified indirectly (e.g., a medical insurance number, your position in a company or by means of a study code assigned in a clinical trial).

In some countries, Personal Information may also include information such as medical device serial numbers, biological samples, IP addresses or information relating to a company ("legal person").

"Sensitive Personal Information" is a subset of Personal Information that requires a higher level of protection. Such information may include racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, social security or insurance information, criminal charges, conviction / sentence, or a person's sexual orientation, or health information. Data elements that make up Sensitive Personal Information may vary by country and local law should be consulted. Associates should check with their legal function or Data Privacy Officer for guidance.

References

Your local Data Privacy Officer will provide information regarding your local Data Privacy laws, definitions and requirements through Standard Operating Procedures ("SOPs") specific to your function, guidance, or other controls, and through training. If you have additional questions, contact your local Data Privacy Officer.

2.2 Collect and use Personal Information fairly and lawfully

Principles and Rules

A fundamental principle of Data Privacy requires that Novartis process Personal Information fairly and lawfully. When collecting and using Personal Information, consider how you would like to be treated by a company who is collecting your information and apply relevant laws, regulations and this Policy.

Associates must:

- Collect and use Personal Information only with a legal justification which may include the legitimate business interests of Novartis. For example, some Novartis guidelines or local laws may require explicit consent of the person concerned prior to collecting Personal Information (e.g., informed Consent for clinical research).
- Notify persons about how their Personal Information will be used prior to collecting the information.
- Collect only the Personal Information needed for a specific business purpose.
- Use Personal Information only for the specific business purpose described in the Privacy Notice or Consent form or in a way that the person would reasonably expect.
- Use Personal Information in ways that do not have an adverse effect on the person concerned unless such use is justified by law.
- Anonymize or Pseudonymize Personal Information when possible or appropriate.

Definitions

"Anonymization" means the process by which Personal Information is irreversibly stripped of all identifiers and can no longer be linked back to the person. Once this is done, it is no longer considered Personal Information.

"Consent" means any freely given, specific, revocable and informed indication of the person's agreement to the processing of his/her Personal Information.

"Explicit Consent" means that an individual is clearly presented with an option to agree or disagree with the collection, use, or disclosure of Personal Information and clearly indicates their choice.

"Privacy Notice" means an oral or written statement that individuals are given when Personal Information about them is being collected. The Privacy Notice describes who is collecting Personal Information, why Personal Information is being collected, how it will be used, shared, stored and any other relevant information of which the person should be aware. Oral notices may need to be recorded to establish evidence that notice was provided to the person and these requirements should be stated in local SOPs, if applicable.

"Pseudonymize" means replacing a person's name and most other identifying characteristics with a label, code or other artificial identifiers in order to protect against identification of the person. Pseudonymized data is still considered Personal Information.

References

Guideline on Anonymization of Personal Information for Secondary Use

2.3 Manage and maintain Personal Information responsibly

Principles and Rules

Responsible management of Personal Information is required to protect privacy rights and comply with Data Privacy laws.

Each Associate is accountable for compliance with Data Privacy obligations related to Personal Information. Associates who collect, use and/or maintain Personal Information must take the appropriate steps to:

- Keep Personal Information accurate and up to date throughout the information lifecycle (i.e., from collection to destruction).
- Safeguard Personal Information so that it is not shared with others who do not have a valid business reason to access the information. For example, there would not be a valid reason for clinical research data to be shared with marketing associates for marketing purposes.
- Comply with Novartis information security policies and procedures when processing Personal Information.
- Prevent the misuse of Personal Information for a purpose that is not compatible with the original purpose for which it was collected.
- Ensure Traceability of Personal Information throughout its lifecycle.
- Keep Personal Information only as long as necessary for the specific purpose or as required by law. Consult your records retention schedules for specific timeframes for maintaining Personal Information.
- Report any Data Privacy Breach to the Information Governance Management Security function via ask.igm@novartis.com

Novartis has designated a Global Data Privacy Office which is accountable for developing, communicating, and providing training on the overall Novartis privacy program which can be found on the Group Data Privacy Intranet site. Novartis has further designated local Data Privacy Officers who are accountable for advising on local privacy related matters, and for implementing local Data Privacy controls.

Definitions

"Data Privacy Breach" means any unauthorized disclosure, acquisition, access, destruction, or alteration of, or any similar action involving Personal Information, or any other incident where the confidentiality of Personal Information may have been compromised.

"Traceability" follows the lifecycle of information to track all access and changes to Personal Information and locations of the Personal Information. It helps Novartis demonstrate transparency, compliance and adherence to regulations.

References

IGM Policy Framework
Data Privacy Intranet site

When in doubt whether Personal Information may be used for a purpose different from the purpose for which it has been collected, or in case of any other question related to the management of Personal Information, please review your local SOPs, guidance, other controls, or contact your local Data Privacy Officer.

2.4 Know how to disclose Personal Information to Third Parties and other Novartis affiliates

Principles and Rules	Personal Information may be shared with other Novartis affiliates, government agencies and Third Parties for legitimate business reasons or as otherwise allowed or required by law. Associates who share Personal Information with Third Parties must obtain assurance that the Third Party has the ability and intention to protect Personal Information, consistent with the standards and principles contained in this Policy. This may be done through Third Party due diligence, risk assessments, and/or a contract. A processing agreement is required whenever a Third Party is provided access to Personal Information in order to Process such Personal Information on behalf of Novartis. In addition, a similar agreement is required when one Novartis affiliate Processes Personal Information on behalf of another Novartis affiliate. These agreements may take the form of contracts between Novartis affiliates, or Novartis standard contracts with Third Parties. All agreements must include the Data Privacy principles and processing instructions. Based on risk assessments conducted on Third Parties, appropriate technical safeguards (e.g., encryption) or other remedial measures need to be provided for by contract to ensure adequate protection of Personal Information.
Definitions	"Process" means any operation or set of operations performed upon Personal Information. This definition includes, but is not limited to, collection, recording, organization, storage, retrieval, use, disclosure, anonymization, pseudonymization or deletion. "Third Party" is any person, including a legal entity, with whom Novartis interacts and that is not a Novartis company or Associate.
References	Internal Processing Agreement Questions regarding requirements for the disclosure of Personal Information to Third Parties should be addressed to your local Data Privacy Officer.

2.5 Know how to transfer Personal Information across borders

Principles and Rules

In many instances, the use of Third Parties will also involve the Transfer of Personal Information across country borders. Also, many business processes require the Transfer of data within Novartis Group of Companies.

When you Transfer Personal Information across borders to Third Parties you need to :

- Determine if you have a legitimate justification for the Transfer of Personal Information (e.g., valid business reason);
- Follow your local SOPs for any other local legal requirements (e.g., notice to the individual, notification to data protection authorities, use of contractual safeguards such as, e.g., EU model clauses).

The Transfer of Personal Information from Novartis Companies operating as Controllers in the EEA or Switzerland to other Novartis Companies established outside the EEA and Switzerland are permitted under the Novartis Binding Corporate Rules. For Transfers from other countries within the Novartis Group of Companies, consult your local SOP.

Definitions

"Third Party" is any person, including a legal entity, with whom Novartis interacts and that is not a Novartis company or Associate.

"Transfer" means any disclosure of Personal Information by someone other than the person to whom the personal data belongs. The term "Transfer" may include the physical movement of Personal Information or the provision of access to Personal Information.

References

Frequently Asked Questions (FAQ) on Data Transfers across Borders
Binding Corporate Rules booklet
European Economic Area (EEA) countries
Adequate countries
EU Model Clauses and Swiss Transborder agreement

Questions regarding requirements for data Transfers across borders should be addressed to your local Data Privacy Officer.

2.6 Right of Access, Rectification, Cancellation and Objection

Principles and Rules	Affiliates need to implement processes in applicable SOPs to ensure an appropriate and lawful response to persons who exercise their individual rights to 1) know what Personal Information is being Processed about them, 2) object to processing, and/or 3) request correction, erasure or blocking of their Personal Information. Associates who collect Personal Information or develop systems that hold Personal Information must ensure that these rights can be executed within a reasonable timeframe or as required by local law.
References	These rights may have certain restrictions for regulatory or legal reasons; if so, they should be outlined in local SOPs.

3. Implementation

3.1 Training and Awareness

Associates must familiarize themselves with this Policy and any other privacy related Novartis documents developed by either the Global Privacy Office or Information Governance Management. Each Associate must participate in training that may be given from time to time.

3.2 Reporting Potential Misconduct/Non-Retaliation

Any Associate, who learns of a potential violation of applicable laws and/or this Policy, is required to report his or her suspicion promptly in accordance with the section of the Novartis Code of Conduct entitled "How to report potential misconduct".

Associates who report potential misconduct or who provide information or otherwise assist in any inquiry or investigation of potential misconduct will be protected against retaliation.

3.3 Breach of this Policy

Breaches of this Policy may lead to disciplinary and other actions up to and including termination of employment or contract (for Third Parties).

3.4 Standard Operating Procedures

If required due to more stringent local laws or regulations or if processing Personal Information covered by the Novartis Binding Corporate Rules, Country organizations should implement this Policy through local functional Standard Operating Procedures ("SOP"), guidance, or other appropriate controls. The local SOPs must be reviewed periodically or ad hoc to comply with changes in local laws, and updated as necessary. The Country Data Privacy Officer is responsible for coordinating the development and distribution of such SOPs, guidance, or other controls to all local Novartis divisions.

3.5 Responsibilities and Implementation

It is the responsibility of every Novartis manager to adhere to this Policy within his or her area of functional responsibility, to lead by example, and to provide guidance to those Associates reporting to him or her.

All Associates are responsible for adhering to the principles and rules set out in this Policy.

The owner of this Policy on the Protection of Personal Information is the Global Privacy Office (global.privacy_office@novartis.com).