NOVARTIS | Reimagining Medicine

Data Privacy Policy

Novartis Global Policy

Document Owner: Global Data Privacy

Version: 4.0

Ethics, Risk & Compliance
Global Data Privacy

Contents

1. Introduction

1.1. Purpose

Personal Information (sometimes called Personal Data) is any information related to a real person, such as a patient, a healthcare provider, a Novartis associate, and other individuals. It may also include information about a browser or device used by one of these individuals.

Novartis recognizes that all people have fundamental privacy rights and freedoms, and the company is committed to responsibly using Personal Information as reflected in the Code of Ethics [1].

To help the company protect these rights and freedoms, recognize when you are collecting, handling, sharing or otherwise using Personal Information and apply the five data privacy principles below to guide you.

This policy establishes company data privacy principles globally. However, privacy laws vary from country to country. Where local laws, regulations, or industry codes are more stringent than this policy, follow local requirements, and in case of doubt, reach out to the privacy office.

1.2. Scope and Applicability

1.2.1. Scope

The scope of this policy is global.

1.2.2. Applicability

This policy applies to all associates and contractors with access to Novartis systems, as well as third parties who are contractually required to follow this policy.

1.3. Roles and Responsibilities

Role	Responsibilities
Associates	Must comply with this policy when handling Personal Information on behalf of Novartis
Contractors with access to Novartis systems	Must comply with this policy when handling Personal Information on behalf of Novartis
Third parties who are contractually required to follow this policy	Must comply with this policy when handling Personal Information on behalf of Novartis
Global Data Privacy	Owns and maintains this policy

2. Principles

2.1. Be transparent

Describe in clear and simple language what Novartis does with Personal Information and communicate this at an appropriate time. By doing so, Novartis builds trust with patients, healthcare providers, and with society.

2.1.1. Requirements

- Explain what Personal Information will be collected, who is collecting it, why it is being collected, how it will be used, and who it will be shared with
- Communicate this at the time Personal Information is collected (if possible) in a format that is easily accessible
- Being transparent may involve providing a link to an online Novartis privacy notice (such as a notice contained in the Novartis Privacy Hub located at www.novartis.com/privacy or on a local corporate website)
- Consider whether it is appropriate (or required) to empower individuals with choices regarding what information they provide and how Novartis uses it

2.2. Collect only what is necessary

Collect the minimum necessary Personal Information to further a specific, and legitimate, business purpose.

2.2.1. Requirements

- Identify the specific purpose(s) for collecting Personal Information
- Ensure Personal Information is collected only for such purposes.
- Consider whether the business purpose could be achieved with less Personal Information, and only collect the minimum data needed

2.3. Use responsibly

Use Personal Information responsibly, meaning only in ways compatible with the purposes for which it was collected, and as communicated. This includes ensuring that the company only transfers such information across country borders where it is appropriate to do so.

2.3.1. Requirements

- Use Personal Information only in ways consistent with any notice presented
- Include appropriate data privacy protections in contracts where Personal Information will be handled by a third party
- When handling sensitive Personal Information, such as health data, recognize that enhanced data privacy protections may be needed
- Honor individuals' preferences and privacy requests, including to access, delete, or correct their Personal Information, subject to local laws and requirements.
- If local law allows transferring Personal Information across country borders, follow local requirements when transferring to third parties
- Be aware that when Personal Information is sent from Novartis in the European Economic Area (EEA) or United Kingdom (UK), and received in another Novartis location, the Novartis Binding Corporate Rules apply [2] [3]

2.4. Protect and be vigilant

Follow applicable Novartis information security policies and guidelines. Be on the lookout and immediately report any unintended use or disclosure of Personal Information.

2.4.1. Requirements

- Classify Personal Information and store it according to the Information Security Risk Management (ISRM) policy[4]
- Prevent Personal Information from unintended modification, use, or disclosure by complying with ISRM policies and guidelines, available at go/isrm
- Keep Personal Information accurate and up to date
- Report any security incident or other unauthorized sharing, receipt, or handling of Personal Information at go/securityincident

2.5. Retain only as long as necessary

Collect Personal Information only for specific business needs. Once the Personal Information is not necessary, it should not be kept unless needed to comply with legal obligations

2.5.1. Requirements

- Follow records retention schedules at go/grrs for specific timeframes for maintaining Personal Information
- Delete Personal Information when no longer needed (unless otherwise required for legal reasons)
- In some situations, anonymization may be used as an alternative to deletion

3. Internal Controls

Internal controls for this policy are stored in the Novartis Internal Control Register at ‘go/controlregister’.

4. Breach of this Policy

Breaches of this policy can result in remedial, corrective, or disciplinary actions up to and including termination of employment. Actual or suspected incidents of misconduct should be reported to the SpeakUp Office. Novartis guarantees non-retaliation and confidentiality, to the extent legally possible, for good-faith reports of such breaches.

5. Exceptions

There are no exceptions to this policy.

6. Adaptations

There are no adaptations to this policy.

7. Definitions

Term	Definition
European Economic Area	The Member States of the European Union (EU) and three countries of the European Free Trade Association (EFTA) (Iceland, Liechtenstein and Norway).
Personal Information	Any information related to a real person, such as a patient, a healthcare provider, a Novartis associate, and other individuals. It may also include information about a browser or device used by one of these individuals.

8. Abbreviations

Abbreviation	Description
EEA	European Economic Area
ISRM	Information Security & Risk Management
UK	United Kingdom

9. References

Reference Number	Document Name
1	Code of Ethics
2	Novartis Binding Corporate Rules
3	Novartis Binding Corporate Rules (UK)
4	Information Management Policy