Data Privacy, Digital and Artificial Intelligence Compliance (DPDAI)

Ethical Use of Data and Technology Policy

Novartis Global Policy

Version: 2.0 Public

NOVARTIS | Reimagining Medicine

Contents

1. Introduction

1.1. Purpose

Data and Technology are powerful assets that the company uses to improve and extend people's lives but can cause harm if misused. As stated in our Code of Ethics and emphasized in the Doing Business Ethically Policy , Novartis is committed to use Data and Technology ethically. Through the ethical use of Data and Technology, Novartis maintains trust with patients, healthcare professionals, its Employees, and society.

This Policy defines high level principles that are broadly applicable across Novartis. These principles are illustrated with several examples (non-exhaustive) of how the principles should be interpreted and applied in practice.

Risk and compliance management processes are generally implemented at an enterprise level for Data and Technology management and use.

1.2. Scope and applicability

This Policy is applicable to all Novartis Employees and contractors who use Data or Technology at Novartis, and any third parties who are contractually required to follow this Policy.

1.3. Exceptions

Exceptions to this Policy are not permitted.

1.4. Adaptations

There are no adaptations to this Policy.

1.5. Roles and responsibilities

Role	Responsibilities
Employees	• Must comply with this policy
Contractors	• Must comply with this policy
Third parties who are contractually required to follow this Policy	• Must comply with this policy
ERC Data Privacy, Digital and Artificial Intelligence Compliance (DPDAI)	• Owns and maintains this policy

2. Principles

2.1. Respect humanity

Respect humanity and maintain trust with society through deploying and using Data and Technology in ways that promote fairness and inclusion, respect human rights, and benefit patients and society.

Examples of how to apply in practice:

- Use Data and Technology in ways which are inclusive and do not discriminate against any individuals or groups. Take extra care when using Data related to race, gender, ethnicity, sexual orientation, political or religious beliefs, or similar characteristics.
- Use the internet and digital engagement tools in ways that are transparent, honest and respect the rights of others, including cultural norms, where applicable.

- Design and deploy Data and Technology solutions considering the needs of all individuals, including different abilities, languages, and backgrounds.
- Ensure AI training Data is representative and free from bias that could lead to discrimination against certain groups or individuals.

2.2. Be transparent and collect fairly

Describe in clear and simple language why and how Novartis collects Data and what Novartis does with Data and Technology.

Examples of how to apply in practice:

- Be transparent when collecting Personal Data and explain why and how it is being collected, used, and shared.
- Collect the minimum Personal Data needed to fulfill a specific business purpose.
- If posting on social media, disclose any affiliation with Novartis when the topic or content relates to Novartis and/or healthcare.
- When deploying AI Systems, ensure that users are informed that AI is involved and its purpose.

2.3. Use responsibly

Use Data and Technology responsibly and take accountability for the appropriate management and protection of Data and Technology in line with your scope of responsibility.

Examples of how to apply in practice:

- Safeguard Data against unauthorized access, breaches, and cyber threats through use of Novartis authorized systems to collect, share and store Data. Only use these systems for business purposes (unless specifically permitted).
- Use Personal Data only for the purpose for which it was collected or agreed upon by the individuals involved.
- Only share Data with authorized parties, for legitimate business purposes, and with appropriate contracts in place. Protect and ensure the responsible and ethical use of any shared Data, and comply with Novartis and third parties intellectual property rights.
- Be mindful as an Employee when posting, liking, sharing, or tagging on social media as it may affect Novartis and its reputation.
- Retain records following the Novartis global retention schedule. Delete Data once it is no longer needed to support business activities.
- Obtain permission to use Data legitimately and pay attention to any related rights, e.g. copyrights and trademarks in relation to use of images, videos or other content sourced from third parties.

2.4. Protect Data and Technology

Apply risk-based security to protect and ensure the confidentiality, integrity and availability of Data and Technology throughout its lifecycle. Prevent Data loss.

Examples of how to apply in practice:

- Ensure Data is kept accurate at every stage of its lifecycle. Apply the different business, security and compliance requirements for different types and classifications of Data – such as business information, Personal Data, and GxP Data.
- Apply security, encryption and access control based on data classification and where possible as part of system design or configuration. Apply additional protection and monitoring for more sensitive Data.
- Remain vigilant and be on the lookout for potential information security threats and vulnerabilities especially when engaging online.
- Ensure that Novartis documents and information are protected from going outside the company in an unauthorized way. Do not retain, take, remove, copy, download, forward, email, use, or disclose any Novartis information inappropriately.

- Promptly report any suspected or actual incidents such as unauthorized access, Data breaches, or malware infections, as well as any other threats or suspicious activities.

3. Breach of this document

Breaches of this document will result in remedial, corrective, or disciplinary actions up to and including termination of employment.

Actual or suspected incidents of misconduct are to be reported in line with our SpeakUp Policy .

Novartis will take steps to ensure confidentiality and prohibits any form of retaliation against an Employee who raises in good faith a concern about suspected or actual misconduct through any channel, or who cooperates in an investigation of misconduct.

4. Definitions

Term	Definition
AI System	A machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI Systems vary in their levels of autonomy and adaptiveness after deployment. *Note: Definition provided by the Organisation for Economic Co-operation and Development as in "OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449"*
Data	The information that is generated, collected or handled as part of our work. It can be numbers, text, images, audio, videos or details about anything related with our work.
Employee	Refers to anyone who holds an employment contract or other form of written employment agreement with Novartis.
Personal Data	Any information related to a real person, such as a patient, a healthcare provider, a Novartis Employee, and other individuals. It may also include information about a browser or device used by one of these individuals. (Also sometimes referred to as Personal Information).
Technology	Any type of digital technology such as applications, websites, mobile apps, IT infrastructure, or devices such as laptops and mobile phones.

5. Abbreviations

Abbreviations	Description
AI	Artificial Intelligence
DPDAI	Data Privacy, Digital and Artificial Intelligence compliance function within ERC
ERC	Ethics, Risk & Compliance
GxP	Acronym used for the group of good practice guides governing the preclinical, clinical, manufacturing, testing, storage, distribution and post-marketing activities for regulated pharmaceuticals, biologicals and medical devices. Generic term for GMP, GLP, GCP, GPvP, GDP. "x" stands for M (manufacturing), L (laboratory), C (clinical), PV (pharmacovigilance), D (distribution), etc.