Data Privacy Definitions:

Last Updated Date: 15 Sep 2023

'Personal Information' ("PI") is any information through which we can identify an individual. This includes any information about our Patients, Health Care Professionals, Business Partners, Employees, Consumers, and anyone else we interact with. Further, certain types of Personal Information are classified as Sensitive Personal Information ("SPI") – see definition and examples below.

Some examples of Personal Information are:
Name, Initials, Address, Contact Information, Date of Birth, IP Address, Browsing history, Registration/License Number and Employee ID.

'Sensitive Personal Information' ("SPI") is a subset of Personal Information that requires a higher level of protection. While the type of PI classified as SPI may vary from country to country some common examples which may be relevant to us include:

- Health, Medical, Biometric and Genetic information.
- National Identity Numbers, such as Social Security Number, Aadhaar Number etc.
- Ethnicity, Race, Religion and, Sexual Orientation.
- Information related to Offenses or alleged Offenses and Criminal history.

Local Data Protection laws should be considered to identify information classified as SPI and specific considerations to be made while processing such information.

'Consent' means any freely given, specific, revocable, and informed indication of an individual's agreement to the collection, use, processing, or disclosure of his/her Personal Information. This would include explicit consent for any sensitive personal information.

'Data Privacy Undertaking' means a written statement of consent that individuals provide whose personal information are being collected, used or processed by Dr. Reddy's. It entails on how the PI or SPI can be collected by Company and also provides the provider of information the right to view, edit or modify and delete all or some of the Personal Information given by them.

'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.

'Processing' means any operation or set of operations performed on Personal Information, whether or not using automated means, such as collection, recording, organization, storage, retrieval, use, disclosure, anonymization, pseudonymization, erasing or deletion.

'Third Party' is any person, including a legal entity, with whom the Company interacts and that is not a Dr. Reddy's employee.

'Cross-border Transfer' means physical or electronic transfer of Personal Information of one or more individuals outside the borders of the country of origin of such Personal Information. Please note that even the ability to remotely access such Personal Information electronically, from anyone outside of the country of origin is considered as cross-border transfer of Personal Information.
'Data Controller' means a person or an organization which, alone or jointly with others, determines or makes decisions regarding the purposes and means of the collection, disclosure and/or processing of Personal Information.

Unless identified otherwise via the contractual agreement, in most cases where we engage third party service providers, as 'customers' we act in the capacity of a Data Controller, whereas the service providers are the Data Processors. In some jurisdictions Data Controller may be referred to using different terminologies, such as 'Data Fiduciary' in India Digital Personal Data Protection Act., 'Data Operator' in Russian DP law, and 'Personal Information Handler' in China's Personal Information Protection Law.

Data Privacy Definitions:

Last Updated Date: 15 Sep 2023

'Data Processor' means a person or an organization which, collects discloses and/or processes Personal Information on behalf of the Data Controller by itself, jointly or through its sub-contractors The Data Controller continues to remain accountable for ensuring that any processing being carried out by Data Processors is compliant with the applicable Laws.

'Data Subject' is the individual whose Personal Information is collected and/or processed. 'Data Subject' may be referred to using different terminologies, such as 'Data Principal' in India Digital Personal Data Protection (DPDP) Act.

'Data Subject Requests' ("DSR") refer to an individual's request related to their privacy rights under applicable Data Protection laws. Organizations such as ours collecting and/or processing Personal Information also have the obligation to inform data subjects of such rights, how can they exercise them and then honor such requests by implementing their requests. Some of the common rights are:

- Right to be informed about how their Personal Information is collected and used.
- Right to access Personal Information / receive a copy of it.
- Right to rectification or correction of inaccurate Personal Information.
- Right to request deletion of Personal Information
- Right to Opt-out or withdraw consent.

'Privacy Notice' is a public document that an organization makes available to individuals to explain how their Personal Information is collected or processed by the organization. It has two aims: to promote transparency and to give individuals more control over the way their data is collected and processed.

Such a notice must be written in clear and plain language, must be easily accessible and provided/ pointed to at the time of collection of Personal Information, when we are collecting such information directly from an individual. Some of the topics that the notice aims to cover are:

- who is the Data Controller,
- what categories of Personal Information is being collected, how and for what purposes,
- if the information will be shared with third parties and/or transferred across the borders,
- safeguards (technical and organizational measures) in place to protect the information,
- how long will the Personal Information be stored,
- what are individual rights under applicable laws and how can they exercise them, etc.

'Anonymization' is a process of rendering Personal Information or Data anonymous. This is done by removing both direct identifiers (such as name, phone number, email Id) and indirect identifiers (such as date of birth or age, ethnicity, postal codes) of the individual from a dataset in a way that the individual(s) can no longer be identified. Once the data is truly anonymous, in most cases, it is no longer considered Personal Information and therefore will no longer fall within the scope of Data protection laws.

Few other things to note:

- Anonymization does not always reduce the risk of re-identification of individuals to zero. This is dependent on the process adopted and may vary on a case-by-case basis.
- Anonymization is not permanent. With evolving technology landscape and availability of information the risk of re-identification may increase and therefore an ongoing review of such information is important.
- Encryption is not an anonymization technique.
- From business standpoint, the utility of the anonymized data set should be kept in mind before adopting this technique.

Data Privacy Definitions:

Last Updated Date: 15 Sep 2023

'Pseudonymization' on the other hand is a de-identification procedure by which Personal Information identifiers in a data set are replaced by one or more artificial identifiers/code or pseudonyms in such a manner that the data cannot be attributed to a specific data subject or individual without the use of additional information* e.g., replacing patient name with a patient ID and clinical site name with a site Id in the clinical trial world. Pseudonymized information is still considered Personal Data and is therefore in scope of Data protection laws.

*Such additional information that can help identify specific individual should be kept separately with appropriate technical and organization measures in place to prevent unauthorized disclosure or misuse.