PRIVACY POLICY

Effective date: 01/09/2022

This privacy policy describes how Ipca Laboratories Limited collects, uses and store personal information about data subjects in accordance with regulations on the protection of persons with regard to the processing of personal data.

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1. Who are we?

Ipca Laboratories Ltd. (hereinafter referred to as Ipca) is an integrated pharmaceutical company, manufacturing formulations and Active Pharmaceutical Ingredients (APIs) for various therapeutic segments. Ipca has been partnering healthcare globally in over 120 countries.

2. Scope of this policy

Ipca takes the protection of personally identifiable information ("Personal Data") very seriously. This Privacy Policy addresses data subjects whose Personal Data we process in our safety database.

3. Controllership

In the context of this policy, Ipca's Corporate Pharmacovigilance Cell acts as a data processor for the Personal Data we process.

4. Why do we need your information?

Ipca needs to protect and promote public health and patient safety by ensuring that medicines manufactured or marketed by Ipca meet appropriate standards of safety, quality, performance and effectiveness.

Ipca has global safety database to collect and monitor information on suspected safety concerns or incidents involving its medicines. It relies on voluntary reporting of suspected safety concerns or incidents by healthcare professionals and members of the public (patients, users, or carers). Our purpose is to investigate these reports and take any necessary regulatory action in line with regulatory requirements.

The Pharmacovigilance Department of Ipca process personal information to:
• Monitor the safety of our medicines.
• Contact the reporter of the adverse event if further information is required.

• Contact representatives of business partners or other companies which supply the medicines to discuss reported adverse events.
• Check that the same information has not been received multiple times for the same adverse event.
• Responding to inquiries, and/or other requests or questions

However, Ipca is conscious of the duty of confidentiality to patients and reporters.

Whenever we process personal data, we will ensure that we comply with the data protection principles, so that your personal data is:

- processed fairly, lawfully and transparently
- processed for specific and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and kept up to date where necessary
- kept in an identifiable form no longer than necessary for the purpose
- processed securely – we will put in place appropriate technical and organisational measures to safeguard your information

5. Our lawful basis

Our lawful basis for processing your personal data is HIPAA (Health Insurance Portability and Accountability Act) , which allows us to process personal data when this is necessary to perform our pharmacovigilance obligations as a Pharmaceutical manufacturer, subject to appropriate safeguards to protect your rights and freedoms. GDPR (General Data Protection Regulation) certification is in progress for Ipca and will be implemented shortly.

To perform our pharmacovigilance obligations, we require some information about the individual affected. If you are submitting a report about yourself, the information will relate to you and include some special category personal data, such as information about your health or ethnicity.

Ipca has been certified by European Assessment and Certification Ltd., which is accredited by ASIB (Accred Services International Board (Europe) Limited in recognition of the organization’s management system that conforms to the requirements of HIPAA.

6. How do we receive personal data?

We may receive your personal data when:

- when you submit adverse event report by phone, e-mail, fax, mail, or a web form or
- when our business partners, such as pharmaceutical companies, provide them to us

7. What personal data do we collect?

We collect data on the reporter and the individual affected; this will be the same person if you are reporting about yourself.

We may collect the following personal data about the reporter:

- title, first name, last name
- email address
- postal address, fax and telephone number
- job title and organisation details if the reporter is a healthcare professional or manufacturer representative

We may collect the following data about the individual affected:

- at least one of the following characteristics: initials, age, sex, weight, height or a local identifier
- ethnicity
- information about the suspected product and a description of the adverse incident
- health data, including medical history and medications

8. Your rights

If you are a data subject about whom we store personal data, you may have the right to request access to, and the opportunity to update, correct, or delete such personal data. You may also have the right to opt out of having your personal data shared with third parties and to revoke your consent that you have previously provided for your personal data to be shared with third parties, except as required by law. You also have the right to opt out if your personal data is used for any purpose that is materially different from, but nevertheless compatible with the purpose(s) for which it was originally collected or subsequently authorized by you.

To submit such requests, please contact the party that has provided your personal data to us. If you have provided your personal data to us directly or if you want to raise any other questions related to the way we process your personal data, please contact the Data Protection Officer using the information in the Contacting Us section of this policy.

9. Our data processors

We use in house data processors, who provide elements of services for us. They may not share your personal data with any other organisation. All the data are held in our safety database securely and retained permanently.

Any vendor who may receive any personal health information, such as Medical Information Services vendor, a Non-disclosure agreement/Confidentiality agreement is signed with them.

10. How long do we keep your personal data?

We keep your personal data permanently as it is necessary to fulfill the purpose we collect it for, including reporting or legal requirements.

11. Disclosure of your personal data

We will not share your information with any third parties for the purposes of direct marketing.

We may disclose your personal data:

- To the respective regulatory authorities with regard to reports of adverse events
- To the business partners
- To the extent required by law or if we have a good-faith belief that such disclosure is necessary in order to comply with official investigations or legal proceedings initiated by governmental and/or law enforcement officials, or private parties, including but not limited to: in response to subpoenas, search warrants, or court orders
- If we sell or transfer all or a portion of our company's business interests, assets, or both, or in connection with a corporate merger, consolidation, restructuring, or other company change or our subsidiaries or affiliates only if necessary for business and operational purposes

Anonymised reports are shared with drug regulatory agencies where the report is relevant to the work of the department. This is shared to support safety monitoring activities and regulatory decisions.

Whenever any adverse event report is shared to business partners for fulfilling pharmacovigilance obligations, we remove all the person identifiers before sharing the reports.

If we must disclose your personal data in order to comply with official investigations or legal proceedings initiated by governmental and/or law enforcement officials, we may not be able to ensure that such recipients of your personal data will maintain the privacy or security of your personal data.

We will also provide a copy of your report to your healthcare provider where you have requested this.

12. Data integrity & security

Ipca has implemented and will maintain technical, organizational, and physical security measures that are reasonably designed to help protect personal data from unauthorized processing, such as unauthorized access, disclosure, alteration, or destruction.

Our service providers may be located outside of the United States, the European Union ("EU") or the European Economic Area ("EEA") and the United Kingdom. However, we will ensure that these third parties maintain at least the same level of confidentiality and data protection that we maintain for your personal data. We have also signed Non-disclosure/Confidentiality agreement with them. Ipca remains liable for the protection of personal data that we transfer to our service providers, except to the extent that we are not responsible for the event giving rise to any unauthorized or improper processing.

Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, shall be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account shall be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person, to identify the natural person directly or indirectly. To ascertain

whether means are reasonably likely to be used to identify the natural person, account shall be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection shall therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

13. Changes in our privacy policy

We will update this privacy policy when applicable to keep it up to date. If we make any material change to this policy, we will post the revised policy to this web page and update the "Effective" date above to reflect the date on which the new policy became effective.

If any change would result in us processing your personal data for a new purpose, we will inform you before we start using it in the new way.

14. Contacting us

If you have queries or concerns about how Ipca protects and uses your personal data, please contact our Data Protection Officer, Ms. Geeta N. Shanbhag, by email at geeta.shanbhag@ipca.com, by phone + 91 22 6647 4630 or by postal mail at:

Attn: Geeta N. Shanbhag
Corporate Pharmacovigilance Cell
Ipca Laboratories Ltd.,
142-AB, Kandivli Industrial Estate,
Kandivli (West),
Mumbai – 400 067
India