Table of Contents

1.0 Purpose

This Privacy Manual has been compiled so that employees are aware of what types of personal information and other legally protected data ("Personal Data") is processed for subjects, vendors, and the employees themselves. There are various types of data categories to which protection will be provided. As these categories and the policies concerning them may be updated from time to time, please continue to refer to this Manual and the policies noted herein so that you may continue to be apprised of any changes to the information presented.

2.0 Scope

This Privacy Manual applies to all Insys Therapeutics, Inc. and its wholly owned subsidiaries (herein "Insys") employees. All employees must read this Privacy Manual in full. Employees performing data processing tasks for study participants, employees, consultants or vendors are doing so on behalf of Insys as the data controller.

This Privacy Manual is particularly focused on how Personal Data is processed and transferred from the European Union ("EU") as well as Switzerland ("Swiss") to the United States including its territories ("US") in conformity with the EU General Data Protection Regulation (referred to herein as the "GDPR").

3.0 Data Protection Principles

Personal Data relates to a natural individual who can be identified, directly or indirectly, from that data or information. Identification can be by the data or information alone or in conjunction with any other data or information in the data controller's possession or which is likely to come into such possession. The processing of Personal Data of the EU citizens or residents ("Data Subjects") is governed by the GDPR.

The term "processing" includes any operation or set of operations performed on Personal Data, whether or not by automated means, such as collecting, recording, organizing, structuring, storing, retrieving, consulting, using, disclosing, disseminating, adapting or altering, and otherwise making available the data.

GDPR recognizes that non-EU businesses processing Personal Data may be in compliance with GDPR requirements by following contractual provisions contained in the EU Standard Contractual Clauses as required by the EU Directive on Data Protection, as well as certification to the EU-US Privacy Shield and Swiss-US Privacy Shield ("Privacy Shields"). However, the basic principles contained herein apply to processing Personal Data whether transmitted from the US or to the US from any other countries in which Insys does business, such as Canada, Australia, Mexico, Saudi Arabia or Argentina. As various countries may have special rules, they will also be addressed as necessary under applicable local law.

The GDPR provides extensive privacy protections and rights to individuals in the EU. The GDPR applies to any organization operating within the EU, as well as any organizations outside the EU which

offer goods or services to individuals or businesses in the EU. The GDPR applies to Personal Data about individuals (including vendors and employees) located in the EU, regardless of where the data resides. The potential penalties for GDPR non-compliance are severe and may be up to 4% of annual global revenue or 20 million Euros (whichever is greater).

Data Subjects rights regarding personal data

GDPR grants Data Subjects a range of specific rights they can exercise in regards to their Personal Data including:

- Right to access their Personal Data and information about that data, such as uses and location;
- Right to rectification (correction) of any inaccurate Personal Data;
- Right to erasure (right to be forgotten) - this is the right to request their Personal Data be erased where it is no longer necessary for Insys to retain such data;
- The right to withdraw their consent to or restrict the processing of the Personal Data at any time;
- The right to data portability including the right to receive and transfer Personal Data to another party;
- The right, where there is a dispute in relation to the accuracy or processing of their Personal Data, to object to use or further processing; and
- The right to lodge a complaint against Insys with governmental agencies or Data Protection Authorities as provided for in the GDPR.

Data Subjects may exercise their rights to data rectification, erasure, portability, access and/or restricted processing by sending their request to Insys Privacy Team at privacy@insysrx.com.

4.0 Privacy Statement

Insys is committed to conducting its business ethically and in compliance with all applicable laws, guidelines, and policies. Insys has deployed global data protection compliance efforts for the protection of all personal data Insys processes. Insys has elected to adhere to enforcing the GDPR, EU Standard Contractual Clauses, and the Privacy Shields concerning the transfer of personal identifiable data from the European Union and Switzerland to the United States of America.

The term "processing" includes any operation or set of operations performed on Personal Data, whether or not by automated means, such as collecting, recording, organizing, structuring, storing, retrieving, consulting, using, disclosing, disseminating, adapting or altering, and otherwise making available the data.

Insys's adherence to the Privacy Shield policies are subject to the investigatory and enforcement powers of the United States Federal Trade Commission. Insys is potentially liable in cases of onward transfer to third parties of data of EU or Swiss individuals received pursuant to the EU-US and Swiss-US Privacy Shield, respectively.

Insys is Privacy Shield certified with the Department of Commerce ensuring that Insys complies with the EU-U.S. Privacy Shield Framework and the Swiss – U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States, respectively. If there is any conflict between this statement and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov.

Who are we

Insys is a pharmaceutical company that develops and commercializes innovative drugs and novel drug delivery systems of therapeutic molecules that aim to improve patients' quality of life. Insys is developing a pipeline of products intended to address unmet medical needs and the clinical shortcomings of existing commercial products. To learn more about Insys please visit https://www.insysrx.com.

Sources of personal data

Insys business actions include the conduct of global clinical trials, commercial activities related to pharmaceutical drugs and delivery systems, and general business management activities. During the course of conducting these activities, Insys collects personal data pertaining to clinical trial staff and study participants, employees, and vendors.

Types of personal data

The personal information Insys collects may include the following:

- Name and contact information
- Demographics
- Location Data
- Personal Health Information
- Account and/or Payment Information

Use of personal data

Insys is a data controller according to the GDPR, which means that Insys determines the purposes for which, "why", and the means by which, "how", personal data is processed. The personal data of clinical trial staff and study participants is typically used to assess the safety and efficacy of Insys products. Employee and Vendor information is generally used for business purposes such as employment status, work completion, and billing/payment information.

Sharing your personal data

For clinical trial participant Data Subjects, please refer to your clinical trial documentation for more information on third-party vendors who may receive access to your personal information. Additionally, you may send an inquiry to the Insys Privacy Team at privacy@insysrx.com.

For non-clinical trial participant Data Subjects, personal information may be shared with business service vendors, covering areas such as payroll, billing, and employee benefits. Additionally, Insys may share personal information in response to lawful requests by public authorities, including to meet national security, law enforcement requirements, and tax and reporting requirements.

Data protection compliance

Insys complies with its obligations under the GDPR by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorized access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.

Personal data provided to Insys may be stored in data centers in the United States.

Further data processing

Insys will not further process any personal data for a new purpose not covered by existing processing agreements without providing impacted persons with a new notice explaining this new use. Where and whenever necessary, Insys will seek prior consent to the new processing.

Cookies and Website Privacy Practices

The Insys website uses cookies, tracking pixels and related technologies. Cookies are small data files that are served by our platform and stored on your device. When anyone visits Insys' website, Insys does not track Personal Data, names or email addresses. Instead, Insys could track which Internet Service Provider has accessed the site as well as statistics that show the number of site visitors, any requests received and the country the request originated. This information may be used to improve our site.

Confidentiality

Insys treats all material provided to us from our Clinical Trial Staff and Participants, Employees, and Vendors collectively, ("CEVs") as confidential in accordance with current confidentiality agreements.

Confidentiality provisions are required as part of all clinical trials as well as our contracts with all our vendors and employees; each separate entity must sign a confidentiality agreement prior to becoming affiliated or working with Insys. All vendors who will be processing personal data are required to sign the EU Standard Contractual Clauses.

Except as may be required by law or during a registrar or regulatory audit, Insys will not provide this data to a third party without their consent.

Email Correspondence

All emails sent to Insys are routed through data servers in the United States. This means all email correspondence originating outside of the United States with an end destination other than the United States still must travel through the United States before arrival at the desired location.

Limiting use/disclosure of personal information

Data Subjects have choice concerning what personal data is accessed, used or retained by Insys. For business purposes, it is necessary for Insys to maintain certain contact information and/or billing information. Any further questions concerning personal data storage, access, and usage may be discussed with Insys Privacy Team by contacting privacy@insysrx.com.

Access and Correction

Data Subjects may request a copy of the personal data Insys has collected from Insys in accordance with applicable law. Data Subjects also have the right to correct, amend or delete information when it is inaccurate. This information can be corrected and/or discussed with the Insys Privacy Team by contacting privacy@insysrx.com.

Data Integrity

Insys is dedicated to ensuring that all data maintained is accurate, updated, and relevant for the agreed upon use. Insys will take all required steps to ensure the data is accurate, complete and current.

Data Security

Insys has strict physical and logical security procedures to ensure that all electronic and paper records are secured. Insys' information security is managed internally and is routinely audited to ensure conformity with Insys procedures and recommended industry standards such as the Health Insurance Portability and Accountability Act (HIPAA) and GDPR.

Data Retention

Insys will only retain personal data for the timeframe necessary to complete its business purposes, such as through regulatory approval process. Although Data Subjects have the right to request the deletion of personal data pertaining to them, Insys, as permitted by applicable law, will continue to maintain its records in such a way that Insys may retain its historical knowledge and relationships concerning any legal or regulatory inquiries which may later arise. This practice is in the best interests of both parties so that identifying information relating to a matter is accessible but sufficiently discrete.

Privacy complaints

In compliance with the Privacy Shield Principles, Insys commits to resolve complaints about our collection or use of your personal information. Data Subjects with inquiries or complaints regarding our Privacy Shield policy should first contact Insys Privacy Team at: privacy@insysrx.com. Your inquiry or complaint will be responded to within 45 days of receipt.

Insys has further committed to cooperate with the panel established by the EU data protection authorities (DPAs) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved Privacy Shield complaints concerning HR and job-related data transferred from the EU and Switzerland. If you do not receive timely acknowledgment of your complaint from us, or if we have not addressed your complaint to your satisfaction, please contact the EU DPAs and the Swiss FDPIC for more information or to file a complaint. The services of EU DPAs and the Swiss FDPIC are provided at no cost to you.

Under certain conditions, more fully described on the Privacy Shield website, you may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted.

Enforcement

Insys will use its best commercial efforts to ensure that compliance to GDPR and Privacy Shields is maintained and that this document is accurate, comprehensive, and continues to conform to applicable laws and regulations. Insys will verify compliance with data privacy requirements not less than once per year and will document the compliance review.

Insys is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) in GDPR and Privacy Shields compliance.

Onward Transfer to Third Parties

In the context of an onward transfer, Insys has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. Insys would remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Privacy Shield Principles, unless Insys is proven to be not responsible for the event giving rise to the damage.

5.0 Clinical Trial Staff and Participants

Clinical Trial Staff and Participants must receive, consent to, and sign off on the proper clinical trial documents such as the contracts or the Informed Consent Form.

6.0 Employees

Insys stores Personal Data concerning its employees for business purposes such as paying taxes, providing benefits, and issuing payroll payments and any other legal purposes. This information is stored as part of Insys' accounting and administrative systems. The information is secured and only accessible by Human Resources and other applicable departments, applicable managers, and the employees themselves. Data will be deleted from time to time and in accordance with applicable law after Insys no longer needs such information for business use. Employees may have information edited on an as needed basis and may discuss any issues regarding such information with their managers and representatives of the Human Resources department. Except as may be required by law, business practices, or during an audit, Insys will not provide this data to a third party without the consent of the employee.

Generally, Insys makes non-work contact information (cell phone, home phone, and email address) accessible to other employees within Insys for the purposes of emergency contact. Additionally, Insys may post personal information regarding education, experience, and promotions as well as pictures of the employee on its intranet and maintain such information as part of Insys' administrative business purpose. Intranets are secured and have limited access. If an employee wishes to remove such information from being posted in this manner, the employee is required to advise the Human Resources department in writing so that the information can be removed. If an employee requests the ability to edit or change the information on an Insys Intranet site, the employee may do so by sending an email requesting such change to Human Resources.

Employees are not permitted to share subject, study, vendor or employee data with or disclose same to any third party without written consent by an authorized representative of Insys. Any misuse of this data for personal or financial gain is also prohibited.

Insys is obligated to enforce the policies which are explained in this Manual and in the event of any failure by an employee to observe its contractual obligations or any provisions of this document they will be subject to disciplinary action, up to and including termination of employment.

7.0 Vendors

All vendors who receive personal information must receive, consent to, and sign off on the EU Standard Contractual Clauses or Business Associate Agreements as applicable. All vendors who receive personal information must also sign a contract detailing their agreement to observe the requirements described and set forth in this Manual.

8.0 Disclosure / Training

Insys provides annual training regarding this document and data privacy practices to all employees.

Revision History

Revision No.	Reason for Change
0	New Issue