

**PHARMACEUTICAL SECURITY INSTITUTE, INC.**

**Privacy Statement**

The Pharmaceutical Security Institute (“PSI”) is a membership organization principally dedicated to addressing the counterfeiting and distribution of pharmaceuticals in violation of law (“Counterfeiting”) and coordinating as need be with Governments, medical control agencies, and law enforcement and other authorities.

PSI respects your privacy and provides this Privacy Statement to inform you of our Privacy Policy, which sets forth the practices and choices you can make about the way your information is collected and how that information is used.

PSI self-certifies that it follows the requirements of the Safe Harbor as set forth by the United States Department of Commerce on July 21, 2000 (the “Safe Harbor”) with respect to all Personal Data<sup>1</sup> it receives from jurisdictions covered by the Safe Harbor, including the European Union. The Safe Harbor sets forth seven principles, relating to Notice, Choice, Onward Transfer, Security, Data Integrity, Access, and Enforcement and Verification. You can find more information about the U.S. Department of Commerce Safe Harbor Program at <http://www.export.gov/safeharbor>.

**1. Notice**

PSI collects and stores some Personal Data relative to visits to its Web site automatically for statistical purposes and also collects and stores Personal Data that is provided to it for the purposes set forth in this Privacy Statement.

**Information collected and stored automatically**

In order to manage this Web site, PSI may collect some information for statistical purposes. This is standard information which is automatically collected and stored in log files; it does not identify a visitor personally. PSI may use software programs to analyze the data and compile statistics. PSI may use the statistics for such purposes as assessing what information is of most and least interest to visitors as a whole, improving technical design specifications, and

---

<sup>1</sup> This Privacy Policy applies only to “Personal Data” as that term is defined in the Safe Harbor. PSI specifically notes that this Privacy Policy does not apply to public record or publicly available information to the fullest extent permitted under the Safe Harbor. PSI may from time to time elect to apply some or all of the provisions of this Privacy Policy to data or uses of data not within the scope of the Safe Harbor, but in doing so creates no rights to such treatment. In connection with any disputes arising from its collection or use of data, PSI reserves its rights to present any defense not specifically waived in this Policy Statement.

identifying performance or problem areas. The standard information that PSI may automatically collect consists of:

The visitor's domain name and the IP address from which the visitor accesses this Web site.

The type of browser and operating system the visitor uses to access this Web site.

The date and time the visitor accesses this Web site.

The Internet address of the Web site from which the visitor accesses this Web site.

The pages the visitor visits on this Web site.

PSI does not give, sell or transfer to third parties any of the information that it automatically collects, unless it relates to a Web site security matter or it is otherwise required to do so by law.

## **Cookies**

A "cookie" is a file placed on your computer's hard drive or in memory by a web site that allows the web site to monitor your use of the web site, usually without your knowledge. PSI uses no cookies to track Personal Data, but it may use cookies to establish state and flow control for applications accessible over the Web.

## **Security and Consent to Monitor**

For site security purposes, and to ensure that this Web site remains available to all visitors, all network traffic may be monitored in order to identify unauthorized attempts to upload or change information, or otherwise cause damage or conduct criminal activity. To protect the system from unauthorized use and to ensure that the system is functioning properly, individuals using this computer system are subject to having their activities monitored and recorded by authorized systems personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals evidence of possible abuse or criminal activity, system personnel may provide the results of such monitoring to appropriate officials. Unauthorized attempts to upload or change information, or otherwise cause damage to this Web site, are strictly prohibited and may be punishable under applicable law. **Except for visitors who voluntarily provide PSI with personally identifying information, and except for authorized enforcement investigations such as discussed herein, no attempts are made to identify individual visitors to this Web Site or their usage habits while visiting this Web site.**

## **Personal Data Otherwise Provided To PSI**

Personal Data may be collected or provided to PSI about alleged counterfeiting incidents and related activities by telephone, letter, facsimile, e-mail to [psi@psi-inc.org](mailto:psi@psi-inc.org), or other means of communication. PSI uses such Personal Data only for the purposes for which it was voluntarily submitted or originally collected or subsequently authorized by the individual, which purposes

include the collection of data about alleged pharmaceutical counterfeiting and related activities, the analysis of such data, the use of such data or analyses in connection with formulating and implementing anti-counterfeiting strategies and/or communications with governmental regulatory or law enforcement personnel or legal counsel. PSI also may aggregate this information (which may include Personal Data) and disseminate it to identify and report on international trends and to provide general information about pharmaceutical counterfeiting and related law enforcement efforts. Except as stated in this Privacy Policy, PSI does not send any Personal Data to any third party.

### **Secondary Notice**

PSI will notify any individual if at any time PSI adopts a policy to use the individual's Personal Data in a manner other than for which PSI had originally collected or processed such data, as described above, and inform each such individual of the new policy. In such event, any such individual will be given the opportunity to choose (*opt out*) that PSI will not use such data in accordance with the new policy, as set forth in item 2, Choice, below.

### **Inquiries and Complaints**

Any individual who has any additional questions or has a complaint about this Privacy Policy or how PSI applies it with respect to such individual's Personal Data, is encouraged to contact PSI in writing, addressed to:

Data Controller  
PSI  
8100 Boone Boulevard  
Suite 220  
Vienna, VA 22812  
Fax: (703) 848-0164

or by e-mail to:

[psi@psi-inc.org](mailto:psi@psi-inc.org)

The inquiry or complaint needs to include the following information to enable PSI to verify that it originates from you:

Your unique username and password, or if you did not supply PSI with a username and password when you first submitted the information, a physical or electronic signature;

Identification of the individually identifying information to which your inquiry or complaint relates;

Identification of any material that you are requesting that PSI remove or disable access to, and information reasonably sufficient to permit PSI to locate the material;

Information reasonably sufficient to permit PSI to contact you, such as your address, telephone number, and if available, an electronic mail address at which PSI may contact you; and

A statement that the information in the inquiry or complaint is accurate.

## **2. Choice**

PSI uses Personal Data only for the purposes for which it was voluntarily submitted or originally collected or subsequently authorized by the individual. PSI will give the opportunity to any individual about whom Personal Data has been provided to choose (“opt out”) that PSI will not (a) disclose such individual’s Personal Data to a third party except as consistent with the Safe Harbor, or (b) use such personal information for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by such individual.

### **Opt-in Regarding Sensitive Information**

PSI does not generally solicit or collect personal information specifying an individual’s medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the individual’s sex life (collectively “*Sensitive Information*”). PSI will only collect and use Sensitive Information as permitted by the Safe Harbor and, as may be required thereunder, will ask such individual in advance to agree (“*opt in*”) to supply such information.

### **Third Party Data Subjects**

In certain instances, the information collected by PSI may include Personal Data not only about legal entities but also about individuals (“*Third Party Data Subjects*”) who have not voluntarily provided the Personal Data to PSI. The purpose of collecting and retaining data on Third Party Data Subjects is the same as that described above generally with respect to all of the Personal Data collected by or supplied to PSI. So long as such Personal Data pertaining to a Third Party Data Subject is included in an active file for a purpose described in this Privacy Policy, PSI will not notify such Third Party Data Subject, and will deny access to such data by such Third Party Data Subject, as the data are collected, retained and processed exclusively for the purpose of the prevention, investigation or detection of offenses, or the prevention, investigation or detection of legal claims of one or more of PSI’s members.

When personally identifying information of a Third Party Data Subject is no longer included in an active file for a purpose described in this Privacy Policy and PSI decides to retain such information in its inactive files, PSI will notify the Third Party Data Subject (but only if PSI possesses the necessary information enabling it to contact such Third Party Data Subject) and inform that individual as to what personally identifying information it has collected and is retaining about such Third Party Data Subject, and give such individual the opportunity to correct or otherwise amend such information.

### **3. Onward Transfer**

PSI will not generally transfer Personal Data to a third party. PSI may however, freely transfer what otherwise would be Personal Data to a regulatory or law enforcement agency or other third party where consistent with public interest or law enforcement requirements as contemplated in the Safe Harbor. PSI at a minimum would make such a transfer only for the purpose of establishing, exercising, or defending against legal claims, or for the prevention, investigation, or detection of violations of law. Neither PSI nor any of its members has any control over regulatory or law enforcement agencies that may be potential transferees. Applicable law in different jurisdictions may affect the confidentiality of the information voluntarily submitted by an individual to PSI and transferred to such agencies. As a result, PSI cannot make any assurances as to whether or not any such agency will keep such personally identifying information confidential. PSI may also forward Personal Data to its Members as may be in conformity with the Safe Harbor, including without limitation pursuant to an agreement requiring that a Member provide at least the same level of privacy protection as is required from PSI under the Safe Harbor Principles.

### **4. Security**

PSI has taken special measures to assure that Personal Data that it collects or has been supplied to it is retained in a secure manner. PSI warehouses the Personal Data on secure systems with limited access, that are located in controlled facilities. Only authorized users, bound by confidentiality agreements, have access to the data stored by PSI.

PSI has appointed a Chief Security Officer (“CSO”) who is in charge of PSI’s security policy and who monitors compliance with this policy. PSI has also developed an Employee Data Security Directive which is intended to ensure compliance with the requirements of the Safe Harbor and this Privacy Policy.

All employees are prescreened for positions dealing with Personal Data. Those who appear unable or unwilling to comply with that policy will have their access to Personal Data denied.

PSI holds periodic security training and compliance evaluation sessions for all its employees which include a discussion of PSI’s Privacy Policy, awareness of its discipline process, how to take action to protect data and equipment in the event of disaster, and training on PSI’s back-up procedures and methods of safe disposal of data.

### **5. Data Integrity**

PSI seeks to ensure that all Personal Data that it maintains is up to date, accurate, complete and relevant.

### **6. Access to Your Personal Data**

With exceptions permitted under the Safe Harbor, you have the right to access any Personal Data that PSI retains about you in order to correct, amend or delete inaccurate information. In the event that you wish to exercise your right, please contact PSI at [psi@psi-inc.org](mailto:psi@psi-inc.org). In order to be

able to access your Personal Data, you must provide PSI with your unique username and password, or if inapplicable, a physical or electronic signature.

PSI may deny access to Personal Data to any individual, including any Third Party Data Subject, if in PSI's opinion the information about such individual cannot reasonably be separated from the information that relates to alleged counterfeiting and related activities, or any confidential commercial information of PSI's members, or generally when in PSI's opinion such access would interfere with (i) the execution or enforcement of the law, including the prevention, investigation or detection of offenses or the right to a fair trial, or (ii) private causes of action, including the prevention, investigation or detection of legal claims or the right to a fair trial.

In addition, PSI may deny access (i) whenever in PSI's opinion the burden or expense of providing access would be disproportionate to the risks created to the individual's privacy in the case in question, or (ii) when in PSI's opinion the rights of persons other than the individual would likely be violated.

PSI may charge a reasonable fee for providing access to Personal Data.

## **7. Enforcement**

The Safe Harbor Principle relating to enforcement has three components: dispute resolution, verification, and remedies, each of which is a part of PSI's Privacy Policy.

### **A. Dispute Resolution Procedure**

If you have an inquiry or complaint regarding PSI's compliance with the Safe Harbor Principles, you should first contact PSI's Data Controller, informing that person of any specific inquiry or complaint you may have about PSI's collection, retention or usage of your Personal Data. The inquiry or complaint must be in writing and set forth all details enumerated under "Inquiries and Complaints" in item 1 above.

If within ten (10) business days (i) you do not receive acknowledgment of your inquiry or complaint, or (ii) your inquiry or complaint is not satisfactorily addressed, you should then follow the procedure set forth in the following provisions:

1. A party who believes a dispute exists (the "disputing party") shall put such dispute in writing to the other party (the "responding party"). Such writing shall clearly, though as briefly as practicable, state the substance and scope of the dispute, the disputing party's position relative thereto, including legal and factual justifications therefor, the remedy sought, and any other pertinent matters.
2. The responding party who receives such a writing shall respond in writing to the disputing party within ten (10) business days. Such writing shall clearly, though as briefly as practicable, state the responding party's response to each of the items included in the disputing party's writing, and any other pertinent matters.

3. A telephone conference shall be held within ten (10) business days between representatives of the parties having decision-making authority regarding the dispute, to negotiate in good faith a resolution of the dispute.
4. If, within ten (10) business days after such telephone conference, the parties have not succeeded in negotiating a resolution of the dispute, the parties' representatives shall submit the dispute to online mediation by a mediator (the "Mediator") assigned by The International Centre for Dispute Resolution of the American Arbitration Association (AAA). If the Mediator is then unable or unwilling to perform due to a conflict of interest, schedule conflict, or otherwise, the parties will agree to a mutually acceptable neutral person. The fees of, and authorized expenses incurred by, the Mediator, or his replacement neutral, shall be shared equally by the parties.
5. The parties hereby agree to be bound by the rules and procedures of the Mediator, or those of his replacement neutral, as then-existing.
6. The parties agree to mediate in good faith for a minimum period of ten (10) business days from the actual commencement of on-line mediation. If the parties are not successful in resolving the dispute through online mediation, as above, then the parties may agree to submit the matter to binding arbitration, or either party may pursue other available remedies upon ten (10) business days' written notice to the other party specifying its intended course of action.
7. The parties may mutually agree to extend any of the time periods stated herein,
8. The parties agree that the mediation provided for here is a compromise negotiation for purposes of all international, federal and state rules of evidence. The entire procedure will be confidential. All conduct, statements, promises, offers, views and opinions, whether oral or written, made in the course of the mediation by any of the parties, their agents, employees, representatives or other invitees to the mediation and by the neutral, who is the parties' joint agent for purposes of these compromise negotiations, are confidential and shall, in addition and where appropriate, be deemed to be attorney client privileged. Such conduct, statements, promises, offers, views and opinions shall not be discoverable or admissible for any purposes, including impeachment, in any litigation or other proceeding involving the parties and shall not be disclosed to anyone not an agent, employee, expert, witness, or representative for any of the parties. However, evidence otherwise discoverable or admissible in a later proceeding is not excluded from discovery or admission as a result of its use in the mediation. If not entirely enforceable, the parties intend that the court enforce this provision to the extent enforceable by such court.

PSI also is subject to the jurisdiction of the Federal Trade Commission (FTC), a government agency with the mandate to enforce the Federal Trade Commission Act, which among other things prohibits unfair or deceptive acts or practices in or affecting commerce. Commerce on the Internet falls within the scope of this statutory mandate. For further information, see <http://www.ftc.gov/privacy/privacyinitiatives/promises.html>.

## **B. Safe Harbor Verification**

On a periodic basis, but not less frequently than once every year, PSI conducts its own objective Safe Harbor compliance review procedure. PSI verifies that its Privacy Policy, as set forth herein, is accurate, comprehensive, prominently displayed, and completely implemented, including implementation of appropriate employee training and other internal procedures.

PSI complies with the U.S.-EU Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries. PSI has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, and to view PSI's certification, please visit <http://www.export.gov/safeharbor/>. PSI abides by the EU Safe Harbor framework as set forth by the Department of Commerce regarding collection, use, and retention of data from the European Union,

## **C. Remedies**

The sanctions for non-compliance with the Safe Harbor principles range from suspension from the Safe Harbor to the award of damages to individuals for privacy violations. Other sanctions include public notice of non-compliance and injunctions. Persistent non-compliance with Safe Harbor principles may result in the loss of its benefit. These sanctions will be enforced either by the arbitrator (if the parties have agreed to submit the dispute to binding arbitration in accordance with paragraph 6 of the Dispute Resolution Procedures set forth under item 7A above), or, if the individual has filed a complaint with the Federal Trade Commission, the FTC.

Specifically, PSI agrees that the arbitrator (if the parties have agreed to submit the dispute to binding arbitration in accordance with paragraph 6 of the Dispute Resolution Procedures set forth under item 7A above) shall have the authority to issue the following sanctions:

- A. Correction of actions found not to be in compliance with the Safe Harbor;
- B. Correction or deletion of inaccurate Personal Data;
- C. Public notification of the decision and action taken by the arbitrator;
- D. Notification to the US Department of Commerce or any relevant U.S. or European authority of the arbitrator's decision and a request for suspension or temporary removal from the Safe Harbor Certification List due to a failure to comply with the Safe Harbor; and/or
- E. Referral of the matter to the U.S. Federal Trade Commission, US Department of Commerce, or other appropriate governmental agency for enforcement action.

Unless otherwise required by law, sanctions shall not include compensatory or punitive damages.

## **OTHER PROVISIONS**

### **Notice And Procedure For Making Claims Of Copyright Infringement**

Alleged Copyright Infringement: If you believe that material posted on this Web site infringes your copyright, you must submit a notification in writing. To be effective, your notification must include the following:

A physical or electronic signature of a person authorized to act on behalf of the owner of the exclusive right that you claim has been infringed;

Identification of the copyrighted work you claim has been infringed;

Identification of the material that you are requesting that PSI remove or disable access to, and information reasonably sufficient to permit PSI to locate the material;

Information reasonably sufficient to permit PSI to contact you, such as your address, telephone number, and if available, an electronic mail address at which PSI may contact you;

A statement that you have a good faith belief that use of the material in the manner complained of is not authorized by you, or the law; and

A statement that the information in the notification is accurate, and under penalty of perjury, that you are authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Upon receipt of the written Notification containing the information set forth above:

PSI shall remove or disable access to the material that you allege is infringing;

PSI shall forward your written notification to the party who provided the material;

PSI shall take reasonable steps to promptly notify the party who provided the material that PSI has removed or disabled access to the material.

### **Counter Notification**:

If you object to PSI's removal or disabling of access to your material in response to a written notification, you may serve PSI with a Counter Notification. To be effective, a Counter Notification must be a written communication provided to PSI's Designated Agent that includes substantially the following:

A physical or electronic signature of the person submitting the Counter Notification;

Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before PSI removed it or disabled access to it;

A statement under penalty of perjury that the person submitting the Counter Notification has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material;

The name, address, and telephone number of the person submitting the Counter Notification, and a statement that the person submitting the Counter Notification consents to the jurisdiction of Federal District Court for the judicial district in which the person submitting the Counter Notification is located, or if the address of the person submitting the Counter Notification is outside of the United States, for any judicial district in which PSI may be found, and that the person submitting the Counter Notification will accept service of process from the party who provided the original Notification or an agent of such person.

Upon receipt of a Counter Notification containing the information set forth above:

PSI shall promptly provide the party who served the original Notification with a copy of the Counter Notification; and

PSI shall inform the party who served the original Notification that it will replace the removed material or cease disabling access to it within ten (10) business days.

PSI shall replace the removed material or cease disabling access to the material within ten (10) to fourteen (14) business days following receipt of the Counter Notification, **provided** PSI's Designated Agent has not received notice from the party who served the original Notification that an action has been filed seeking a court order to restrain the person submitting the Counter Notification from engaging in infringing activity relating to the material on PSI's Web site.

### **DISCLAIMER**

PSI is not responsible for the content of any off-site pages that are referenced by or that reference to the PSI Web site. PSI is not responsible for any defamatory, offensive, misleading, or illegal conduct of other users, links, or third parties, and the risk of injury from the foregoing rests entirely with the visitor.

Links from the PSI Web site to other sites, or from other sites to the PSI home page, do not constitute an endorsement by PSI. The links are for convenience only. It is the responsibility of the visitor to evaluate the content and usefulness of information obtained from other sites.

All information provided by PSI at this Web site is for the convenience of interested visitors and visitors. The information is based on reports from various third party sources whose credibility and knowledge are unknown to PSI. PSI has not independently verified the accuracy of any information. PSI updates information only as new information is submitted. Individual visitors may use the information as they see fit. PSI does not guarantee the accuracy, completeness, timeliness, or correct sequencing of information, PSI is not responsible for errors or omissions, or for the use of, or results obtained from the use of, the information.

Reference to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply endorsement, recommendation, or favoring by PSI.

### **Modification Of This Web site Privacy Policy And Terms Of Use.**

PSI reserves the right to amend this Web site Privacy Policy and Terms of Use and will alert you that changes have been made by indicating the date they were last updated. Your continued use of this Web site after the Web site Privacy Policy and Terms of Use have been amended signifies that you have agreed to any and all new terms.

### **Contact Information.**

If you have any questions or comments regarding PSI's Privacy Policy, privacy practices or terms of use, please contact PSI at [psi@psi-inc.org](mailto:psi@psi-inc.org).