SUNOVION PHARMACEUTICALS INC.

CORPORATE POLICY

WORKING TITLE: Information Security Policy		POLICY NO: 7.02	
Supersedes: **Policy 7.01 Systems and Confidential Information Policy**	**Approval:** **Corporate Policy Review Committee (CPRC)**	**Date Issued:** **January 5, 2012**	**Page: 1of 9**

Section 1. PURPOSE:

Sunovion recognizes its obligation to ensure the confidentiality, integrity and preservation of company data, both electronic and in all other forms. The purpose of this Policy is to provide guidance related to Sunovion Pharmaceutical Inc.'s procedures ("Sunovion" or "Company") that govern those administrative, technical and physical controls, which the Company has established for the purpose of ensuring the security of Sunovion information

Section 2. DEFINITIONS:

"**Confidential Information**" means all non-public scientific, technical, financial, business or other information or data owned, possessed or used by Sunovion, whether or not labeled "Confidential," including, but not limited to, (a) information about Sunovion's products, customers, partners, and business operations and strategies, (b) deliverables, records and materials, (c) financial information, forecasts, and personal information, (d) information disclosed to others on behalf of Sunovion, (e) all information of third parties that Sunovion has an obligation to keep confidential, (f) prescriber data; and (g) protected health information.

"Protected Health Information" is defined in alignment with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and includes any individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

"**Personal Information**" is defined as a person's first name and last name or first initial and last name, in combination with any one or more of the following data elements that relate to such person: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that personal information shall not include information that is lawfully

obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

"**WISP**" is defined as Sunovion's Written Information Security Program, which is comprised of this Policy, all related SOPs, work instructions and training governing Information Security.

"**Company Electronic Systems**" is defined as all Sunovion owned computers and telephones, including mobile communications devices and all data transmitted on such devices, electronic mail, voicemail, networks, internet access and other Sunovion electronic systems including the Sunovion Intranet (Source)

Section 3. APPLICABILITY AND RESPONSIBILITIES:

Compliance with Laws

Sunovion's Information Security Policy is intended to and shall comply with all applicable federal and state laws governing information security.

This Policy pertains to all US Sunovion employees, DSP employees working at or for a US Sunovion facility, contractors, consultants and vendors which are contracted to provide services to Sunovion ("**Covered Personnel**").

Key departmental roles and responsibilities are detailed below. Each department will determine their own processes in accordance with this Policy and document the same in SOPs and Work Instructions.

Compliance Department

Ensure and oversee the following:

- The information security measures outlined in this Policy are formulated, promoted and executed, as applicable
- All Covered Personnel receive adequate and effective training on this Policy
- **WISP** safeguards are tested annually, or more frequently, if there is a material change in business practices that may require enhanced security or integrity controls for records containing **Personal Information**
- Required notifications to government agencies or individuals in the event of a breach of security or material violation of this policy

IT Department

Develop, implement and maintain the following:

- Appropriate security controls related to computer hardware, software and system access to protect Company information

- Appropriate systems and procedures to facilitate the secure transmission of **Confidential Information** between Sunovion and authorized third parties.

- Policies and procedures around logical and physical security measures

- Procedures and protocols in partnership with the other departments which ensure Sunovion's ability to secure and safeguard electronic **Confidential Information**

- Information Security training programs in cooperation with Legal, Corporate Compliance, HR and Sunovion's Director of Records and Information Management

Human Resources Department

Ensure and oversee the following**:**

- Notification of all policies & procedures associated with the on-boarding and termination of Covered Personnel are provided for Managers to follow in accordance with this policy, including the collection of all data, in any form, all keys, keycards, access devices, badges, company IDs, et cetera, are surrendered to the hiring manager at the time of termination. This includes all data in possession at the time of termination, stored on any portable device and any media or device used by the terminated employee.

- The signatory process on the Company's Invention, Non-Disclosure and Personal Conduct Agreement from all Sunovion employees

- For temporary workers, the on-boarding and termination process is managed by a third-party, "Temporary Services" on-site Representative where the Rep works in conjunction with the Sunovion manager to collect all of Sunovion materials prior to their departure.

Department Managers

Ensure and oversee the following**:**

- The proper notification to Human Resources when an employee is terminated, especially in the field

- The collection of all data, in any form, in conjunction with the Company's employee termination process. This includes all data in the Company employees' possession at the time of termination, stored on any portable device and any media or device owned by the terminated employee.

- The collection of all keys, keycards, access devices, badges, company IDs, and the like are surrendered to the hiring manager at the time of termination

- The proper notification of Human Resources, Legal, and/or Information Technologies if an information security breach occurs, or is suspected to have occurred.

Legal Department

The Legal Affairs Department is responsible for ensuring that any third party provider contracts include applicable data protection language, including but not limited to, obligations that:

1. Data disclosed or passed through a particular contract is used solely for the purposes specified under the contract.

2. The third party provider has an information management security program that complies with all applicable federal and state laws, rules and regulations.

Section 4. GENERAL:

The Company collects **Confidential Information** in order to accomplish its business transactions or to comply with any and all federal and state laws, rules and regulations.

The Company also creates, maintains and stores **Confidential Information** in conjunction with normal business processes that is organizational information not intended to be disclosed outside the context of the company or organization responsible for that information.

Department heads are responsible to ensure that SOPs and Work Instructions are developed and adhered to for all processes and procedures that encompass the handling of **Confidential Information** within their department. Access to records containing **Confidential Information** shall be limited to those Covered Personnel whose duties, relevant to their job description, have a legitimate need to access said records, and only for this legitimate job-related purpose.

Written and electronic records containing **Confidential Information** shall be retained and securely disposed of at the earliest opportunity consistent with Sunovion's Records Retention Schedule and RIM Policy or legal hold requirements.

The Company maintains a Written Information Security Program **(WISP)** which is reviewed annually by Corporate Compliance and Information Technologies, or whenever there is a material change in business practice that may affect the security or integrity of **Confidential Information**.

The Company reserves and will exercise the right to review, audit, intercept, access, and disclose all data and communications on **Company Electronic Systems** and services at any time, with or without notice, for any purpose, including to ensure the security of company data. Company employees should have no expectation of privacy when using **Company Electronic Systems**.

Any on-site visitor or vendor not covered under the Invention, Non-Disclosure and Personal Conduct Agreement must always be escorted by a Sunovion employee

4.1 Information Use, Controls and Audit

4.1.1 Confidential Information Use

Company employees and former employees are prohibited from publicly disclosing, including, but not limited to, by way of Company Systems, the Internet and Social Media sites, any **Confidential Information** obtained during the course of their employment.

Confidential Information shall not be removed from the business premises in electronic or written form absent legitimate business need and use of appropriate security measures, as described in this Policy.

4.1.2 Confidential Information Controls

Departmental

The appropriate department head or responsible employee shall ensure that access to **Confidential Information** is restricted to approved personnel.

Only department heads and authorized Company employees are assigned keys to locked storage and allowed access to confidential paper files. Individual confidential files will be assigned to Company employees on a need-to-know basis by the department head.

Covered Personnel

All Covered Personnel shall use best efforts to identify **Confidential Information** as such by using an approved disclaimer, stamp or other mark on applicable paper and electronic documents and e-mail messages. Failure to identify Confidential Information disclosed orally, visually or in writing with an appropriate proprietary stamp or legend shall not negate the confidential nature of such information, but identifying such information in a writing marked “Confidential Information” shall conclusively demonstrate that the disclosing party considers such information to be “Confidential Information.”

All Covered Personnel are required to secure paper files containing **Confidential Information** in their work area when they are not present.

All Covered Personnel are responsible to protect the confidentiality and integrity of any electronic information stored on all forms of removable media.

All Covered Personnel should not reveal to anyone any password used in conjunction with **Company Electronic Systems** at any time, except on a limited, need-to-know basis, for instance, as required for IT system support.

Upon termination of employment, individuals must return all Company property and equipment, including items used in connection with **Company Electronic Systems**, and shall disclose to their supervisors or a manager in Information Systems Security all passwords used in connection with such systems.

Access to electronically stored records, including those containing **Confidential Information**, shall be limited to those Company employees having an authorized and unique login ID. Department heads and/or managers shall make all requests for login ID or access to electronic systems to Information Technologies or the designated system administrator. All such requests shall be made in writing and appropriately documented.

IT Department

The IT Department has established secure user authentication protocols which control User ID and other identifiers; assigns passwords in a manner that conforms to accepted security standards, and applies use of unique identifier technologies.
All employees' Active Directory passwords are changed at regular intervals.

Physical Access to computers, servers, data centers, document files, offsite records storage, etc. is governed by the established security controls and provided to authorized personnel only

A terminated Company employee's physical and electronic access to all systems and **Confidential Information** shall be restricted at the time of termination. This includes computer access, remote electronic access, voicemail, internet, e-mail and access to paper files. Please see the **Records Management and Retention Policy 6.01** for more information.

All computers have a reasonably up-to-date version of security software, including but not limited to anti-virus, anti-spyware and anti-malware software, installed and active at all times.

Laptops, magnetic tape media, and data transmissions containing **Personal Information**, use encryption to further protect the integrity and security of such information.

Third Party Service Providers

Any third party provider that receives, stores, maintains, processes, disposes or otherwise is permitted access to **Confidential Information** must adhere to this Policy and must also have policies and protocols in place to prohibit unauthorized access to or acquisition of Sunovion's **Confidential Information**.

4.1.2.1 **International Data Transfer**

In regards to international data transfer, if requested by Sunovion, any third party provider shall demonstrate and verify its compliance with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50, and the applicable member state laws implementing such directive ("EU Directive").

If further requested by Sunovion in order to enable the Company to comply with any applicable privacy or data protection law, the third party provider shall execute the model contract in a form acceptable to the European Commission on the basis of Article 26(4) of the EU Directive, to offer sufficient data protection

safeguards, in relation to any transfer of Personal Data out of the European Economic Area, unless, in the case of a transfer of Personal Data to the United States, Vendor has certified its adherence to the Safe Harbor negotiated by the United States Department of Commerce and the European Union, and that adherence encompasses the Personal Data which are the subject of the transfer.

All Company employees must ensure that confidentiality agreements are negotiated and executed with all third parties before any **Confidential Information** is received, discussed, or revealed, or before any non-Company personnel are allowed access to areas or materials from which knowledge could be obtained.

Covered personnel must ensure that all **Confidential Information** shared with any third-party is encrypted before transmission or transmitted by encrypted means.

Company employees are responsible to ensure that sharing of **Confidential Information** with any third party is compliant with this and all applicable Company policies and procedures.

4.1.3 Confidential Information Review and Audit

Sunovion Internal Audit

Each department that possesses confidential information should perform periodic reviews of the implementation of this Policy, in partnership with IT, under the oversight and guidance of the Chief Compliance and Ethics Officer.

Departments which are operating under SOX and CMR 17 regulations will perform periodic audits of employee access to **Confidential Information** using Access Control reports provided by Information Technologies.

Third Party Audit

The Company shall have the option, and shall develop and maintain appropriate procedures for conducting Information Security assessments and site audits of potential vendors to assess their ability to secure and safeguard the Company's **Confidential Information** from loss or theft and compliance with this Policy and related procedures.

4.1.4 Breach Notification and Incident Management

Company employees must report suspicious or unauthorized use of **Confidential Information** to their manager or the Chief Compliance Officer.

The Company maintains breach notification procedures in accordance with all applicable state and federal regulations, outlining the reporting, tracking and review of the breach or loss of **Confidential Information** and required notifications, if any.

IT maintains an Incident Response Plan which provides for response and tracking of any known breach or loss of Confidential Information, and escalation to Executive Management.

Section 5. OTHER MATTERS:

Amendment

Management reserves the right to amend this policy as appropriate at any time without prior notice, pursuant to Sunovion Corporate Policy 1.0, Corporate Policy and Review Committee (CPRC).

Failure to Comply

EMPLOYEES WHO VIOLATE ANY SUNOVION POLICIES AND PROCEDURES MAY BE SUBJECT TO DISCIPLINARY ACTION, UP TO AND INCLUDING TERMINATION OF EMPLOYMENT.

UNDER MASSACHUSETTS STATE LAW, Any agency or person who violates the provisions of **(this chapter)** GP shall be subject to a civil fine of not more than $100 per data subject affected, provided said fine shall not exceed $50,000 for each instance of improper disposal. The attorney general may file a civil action in the superior or district court in the name of the commonwealth to recover such penalties.
Reporting Concerns

Reports concerning wrongful behavior, violations or suspected violations of this or any other policy, the Code of Conduct and Ethics, law or regulation may be submitted on a confidential basis or may be submitted anonymously through the Sunovion Compliance Hotline as set forth below. Reports of violations or suspected violations of alleged misconduct or wrongful behavior will be maintained as confidential as practicable under the circumstances, and as necessary to conduct a full and fair investigation.

Reporting Hotline Options:

(a) Toll free telephone number. 866-886-1348
(b) Via the internet at: www.ethicspoint.com

Sunovion does not tolerate any form of retaliation or adverse action against any employee who submits a good faith report of misconduct. In addition to these protections, an employee may also avail themselves of the remedies afforded under federal and state law, including the federal "False Claims Act," 31 U.S.C. Sections 3729-3733, the Commonwealth of Massachusetts Whistleblower Protection Act, M.G.L 149, Chapter 185 and the New Jersey Conscientious Employee Protection Act, N.J. Stat. Ann. Section 34:19, Sections 1 to 8.

Cross-Reference to other relevant documents:

Code of Conduct and Ethics

Records Management and Retention Policy

Contracts and Signing Authority Policy

Electronic and Voice Mail Usage Policy

Employee Resource Guide

ITD-0006-02 Logical Security

MA 201 CMR 17.00 Standards for the Protection of Personal Information

PhRMA Code: PhRMA Code on Interactions with Healthcare Professionals

HIPAA: Health Insurance Portability and Accountability Act of 1996 ("HIPAA")