

**Eli Lilly and Company
Vendor Privacy and Security Standard**

Last Revision: May 5, 2008

1. Purpose.

This Vendor Privacy Standard (or "Standard") sets forth confidentiality, security and privacy requirements with respect to Personal Information Processed by Vendor on behalf of Lilly to ensure that the Processing by Vendor is compliant with applicable privacy, security and data protection laws globally and the requirements of Eli Lilly's Global Privacy Program.

2. Definitions. For the purposes of this Vendor Privacy Standard:

(a) "Personal Information" means any information provided by Lilly and/or its affiliates or collected by Vendor for Lilly and/or its affiliates: (i) that identifies, or when used in combination with other information provided by Lilly or Processed by Vendor on behalf of Lilly identifies, an individual; or (ii) from which identification or contact information of an individual person can be derived. Personal Information can be in any media or format, including computerized or electronic records as well as paper-based files. The foregoing notwithstanding, Personal Information does not include the name, business telephone number, business cell phone number, business address, business email address, or internal Lilly identification number of individual Lilly employees.

Personal Information includes (without limitation): (a) a first or last name or initials; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (d) a telephone number; (e) a social security number, tax ID number or other government-issued identifier; (f) an Internet Protocol ("IP") address or host name that identifies an individual; (g) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual; (h) birth dates or treatment dates; or (i) coded data that is derived from Personal Information. Additionally, to the extent any other information (such as, but not necessarily limited to, case report form information, clinical trial identification codes, personal profile information, IP addresses, other unique identifier, or biometric information) is associated or combined with Personal Information, then such information also will be considered Personal Information.

(b) "Processing of Personal Information" (or "Processing") means any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking or dispersed erasure, or destruction.

(c) "Sensitive Personal Information" is a subset of Personal Information, which due to its nature has been classified by law or by Lilly policy as deserving additional privacy and security protections. Sensitive Personal Information consists of:

- All government-issued identification numbers (including US Social Security numbers, Canadian Social Insurance numbers, driver's license numbers, and passport numbers);
- All financial account numbers (bank account numbers, credit card numbers, and other information if that information would permit access to a financial account);

- Individual medical records and biometric information, including any information on any worker or consumer's health, disability, disease or product interests;
- Reports of individual background checks and all other data obtained from a U.S. consumer reporting agency and subject to the Fair Credit Reporting Act;
- Data elements revealing race, ethnicity, national origin, religion, trade union membership, sex life or sexual orientation, and criminal records or allegations of crimes; and
- Any other Personal Information designated by Lilly as Sensitive Personal Information.

(d) "Services" means the particular services that Vendor performs for Lilly under an Agreement.

(e) "Agreement" means the entire contract between the Vendor and Lilly under which the Vendor performs services for Lilly. An Agreement may be formed through the execution of a written contract by both parties, by Vendor's express or implied acceptance of Lilly's purchase order, or by any other means of offer and acceptance of a contract.

3. General Vendor Obligations.

(a) All Vendor's obligations under the Agreement are in addition to the requirements of this Standard, including those that are similar in nature, and Vendor will not Process or otherwise use any Personal Information for any purpose other than performing the Services for Lilly and as instructed by Lilly. In the event Vendor believes that it cannot satisfy its other obligations under the Agreement while complying fully with the requirements of this Standard, Vendor shall notify Lilly immediately and shall not proceed with any act that would violate this Standard until the conflict is resolved.

(b) Vendor shall immediately inform Lilly, in writing:

- of any request for access to any Personal Information received by Vendor from an individual who is (or claims to be) the subject of the data;
- of any request for access to any Personal Information received by Vendor from any government official (including any data protection agency or law enforcement agency);
- of any inquiry, claim or complaint regarding the Processing of the Personal Information received by Vendor; and
- of any other requests with respect to Personal Information received from Lilly's employees or other third parties, other than those set forth in the agreement.

Vendor understands that it is not authorized to respond to these requests, unless explicitly authorized by the Agreement or by Lilly in writing, except for the request received from a governmental agency with a subpoena or similar legal document compelling disclosure by Vendor.

(c) Any Personal Information collected or accessed by Vendor in the performance of the Services contracted shall be limited to that which is necessary to perform such Services or to fulfill any legal requirements. Vendor shall take reasonable steps to assure the integrity and currency of the Personal Information in accordance with document management provisions in the Agreement.

(d) If the Services involve the collection of Personal Information directly from individuals, such as through a registration process or a webpage, Vendor will provide a clear and conspicuous notice

regarding the uses of the Personal Information, which notice shall be consistent with the provisions of the agreement between Vendor and Lilly. However, no terms of use, privacy statement or other provisions presented to individuals via a webpage or in any other manner shall alter the Vendor's obligations or rights under this Privacy Standard or the manner in which the Vendor may use Personal Information.

(e) Vendor shall not transfer the Personal Information across any national borders or permit remote access to the Personal Information from any employee, affiliate, contractor, service provider or other third party unless such transfer or remote access is specifically permitted in the Processing instructions provided to it by Lilly or it has the prior written consent of Lilly for such transfer or access. Lilly has joined the EU-US Safe Harbor program, and Lilly may instruct Vendor to transfer Personal Information from EU member states to Lilly in the U.S.A. based on this authorization mechanism.

(f) Vendor shall cooperate with Lilly and with Lilly's affiliates and representatives in responding to inquiries, claims and complaints regarding the Processing of the Personal Information.

(g) Vendor shall secure all necessary authorizations from its employees and approved subcontractors to allow Lilly to process the personal information of these individuals as necessary for the performance of the contract by Lilly, including information required to access Lilly systems or facilities, the maintenance of individual performance metrics and similar information.

4. Confidentiality of Personal Information.

(a) Vendor must maintain all Personal Information in strict confidence. Vendor shall make the Personal Information available only to its employees and onsite contractors who have a need to access the Personal Information in order to perform the Services. Vendor shall not disclose, transmit, or make available the Personal Information to third parties (including subcontractors), unless such disclosure, transmission, or making available has been explicitly authorized by Lilly in writing. In no event may Vendor provide Personal Information (or any other Lilly information) to a sub-vendor or sub-processor unless that entity has agreed in writing to the terms contained herein, including (without limitation) the provisions regarding security and Lilly audit rights.

(b) When the Vendor ceases to perform Services for Lilly, Vendor shall return all Personal Information (along with all copies and all media containing the Personal Information) to Lilly or shall securely destroy all Personal Information and so certify to Lilly. (If legislation imposed upon the Vendor does not permit the destruction of whole or part of the Personal Information transferred, Vendor warrants that it shall ensure the continued confidentiality and security of the Personal Information and shall not actively Process the Personal Information transferred after termination of the relationship.)

5. Security.

(a) Vendor shall have documented and implemented appropriate operational, technical and organizational measures to protect Personal Information against accidental or unlawful destruction, alteration, unauthorized disclosure or access. Vendor will regularly test or otherwise monitor the effectiveness of the safeguards' controls, systems and procedures. Vendor will periodically identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of the Personal Information, and ensure that there are safeguards in place to control those risks. Vendor shall monitor its employees and contractors for compliance with its security program requirements.

(b) At appropriate intervals or as otherwise requested by Lilly, Vendor will provide a copy of its written privacy and information security policies and procedures to Lilly.

(c) Prior to allowing any employee or contractor to Process any Personal Information, Vendor shall: (i) conduct an appropriate background investigation of the individual; (ii) require the individual to execute an enforceable confidentiality agreement; and (iii) provide the individual with appropriate privacy and security training. Upon request, Vendor shall provide to Lilly a list of all employees and contractors (including former employees and contractors) who have (or have had) access to the Personal Information.

(d) If the Processing involves the transmission of Personal Information over a network, Vendor shall have implemented appropriate supplementary measures to protect the Personal Information against the specific risks presented by the Processing. Sensitive Personal Information may only be transmitted in an encrypted format.

(e) If the Processing involves the handling of any Personal Information at a Vendor facility on in a computer system under Vendor's control, the Vendor shall comply with following specific standards:

- Access Rights: Vendor shall have an effective process to administer access rights. The process shall include the following controls: (i) users and system resources shall only be given the access necessary to perform their required functions; (ii) access rights shall be updated based on personnel or system changes; and (iii) access rights shall be periodically reviewed at an appropriate frequency based on the risk to the application or system. Vendor shall also use effective authentication methods appropriate to the level of risk.
- Access Procedures:
 1. Vendor shall define physical security zones and implement appropriate preventative and detective controls in each zone to protect against the risks of physical penetration by malicious or unauthorized people, damage from environmental contaminants, and electronic penetration through active or passive electronic emissions.
 2. Vendor shall secure its computer networks using multiple layers of access controls to protect against unauthorized access. In particular, Vendor shall: (i) group network servers, applications, data, and users into security domains; (ii) establish appropriate access requirements within and between each security domain; and (iii) implement appropriate technological controls to meet those access requirements consistently, including (for example) firewalls.
 3. Vendor shall secure access to the operating systems and applications. Vendor shall secure remote access to and from its systems by disabling remote communications at the operating system level if no business need exists and/or tightly controlling access through management approvals, robust controls, logging and monitoring access events and subsequent audits.
 - Malicious Code: Vendor shall protect against the risk of malicious code by using anti-virus products on clients and servers; using an appropriate blocking strategy on the network perimeter; filtering input to applications; and creating, implementing, and training staff in appropriate computing policies and practices.
 - Media Handling: Vendor shall control and protect access to paper, film and computer-based media to avoid loss or damage. In particular, for all media containing Sensitive Personal Information, Vendor shall ensure safe and secure

disposal of such media, and secure all media in transit or transmission to third parties.

- Other Controls:

1. Vendor shall ensure that systems are developed, acquired, and maintained with appropriate security controls.
2. Vendor shall identify systems and applications that warrant security event monitoring and logging, and reasonably maintain and analyze log files.
3. Vendor shall exercise its security responsibilities for outsourced operations through: (i) appropriate due diligence in service provider research and selection; and (ii) contractual assurances regarding confidentiality, security responsibilities, controls, and reporting.
4. Vendor shall have an established a disaster recovery/business continuity plan that addresses ongoing access to the Personal Information as well as security needs for back-up sites and alternate communication networks.
5. Vendor shall maintain reasonable and appropriate insurance coverage in relation to the risks associated with the Processing.

(f) Sensitive Personal Information may not be stored on any portable computer devices or media (including, without limitation, laptop computers, removable hard disks or flash drives, personal digital assistants (PDAs) or computer tapes) unless the Sensitive Personal Information is encrypted, or the hard drive that contains the Sensitive Personal Information on the portable computer device or media is fully encrypted.

(g) Vendor shall maintain all necessary documentation to show compliance with this Agreement. At Lilly's request, Vendor shall submit its data processing facilities for audit, which shall be carried out by Lilly (or by an independent inspection company designated by Lilly). Vendor shall fully cooperate with any such audit. In the event that any such audit reveals material gaps or weaknesses in Vendor's security program, Lilly shall be entitled to suspend transmission of Personal Information to Vendor and Vendor's Processing of such Personal Information until such issues are resolved.

(h) Vendor will promptly and thoroughly investigate allegations of any use or disclosure of Personal Information of which Vendor is aware that is in violation of these guidelines, and will promptly notify Lilly in writing of any material violation. Vendor will notify Lilly immediately upon discovery of any unauthorized access to or disclosure of Personal Information. Vendor shall bear all costs associated with resolving a security breach, including (without limitation) conducting an investigation, notifying consumers and others as required by law or the Payment Card Industry Data Security Standard, providing consumers with one year of credit monitoring, and responding to consumer, regulator and media inquiries.

6. Compliance with Laws.

Vendor must stay informed of the legal and regulatory requirements for its Processing of Personal Information. In addition to being limited to satisfaction of the Services, Vendor's Processing shall comply with applicable privacy or security laws and regulations.