Vendor Privacy and Security Standard

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 Standard:

(a) “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.

(b) “Applicable Laws” means any statute, law, treaty, rule, code, ordinance, regulation, permit, interpretation, certificate, judgment, decree, injunction, writ, order, subpoena, or like action of a governmental authority that applies, as the context requires to: (i) the Agreement and this Standard; (ii) the performance of obligations or other activities related to the Agreement; and (iii) a party, a party's affiliates (if any), a party's Subcontractors (if any), or to any of their Representatives. Applicable Laws, includes A) the Health Insurance Portability and Accountability Act of 1996, B) The Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Privacy and Security Rule regulations of HIPAA and the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the HITECH Act and the Genetic Information Nondiscrimination Act (the “Omnibus Final Rule”) and all amendments to and further regulations of the HIPAA and HITECH Acts (collectively, “HIPAA”), C) 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with regard to the processing of personal data and on the free movement of such data, as amended, updated or repealed from time to time (“Directive”), and any implementing, derivative or related national legislation, rule, or regulation enacted thereunder by any EU Member State subject to its jurisdiction as well as the European General Data Protection Regulation (Regulation (EU) 2016/679), when it becomes applicable.

(c) “Data Transfer Program” means Privacy Shield, Swiss-USA Safe Harbor, or any other framework for transferring Personal Information from the EEA or Switzerland to the USA that is approved by the European Commission as providing an adequate level of protection pursuant to Article 25(6) of the Directive.

(d) "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. Personal Information includes: (i) a first or last name or initials; (ii) a home or other physical address, including street name and name of city or town; (iii) 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; (iv) a telephone number; (v) a social security number, tax ID number or other government-issued identifier; (vi) an Internet Protocol ("IP") address or host name that identifies an individual; (vii) 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; (viii) birth dates or treatment dates; or (ix) 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. Regarding data originally collected in the United States of America, 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.

(e) "Privacy Shield" means the EU-US framework of privacy principles agreed on February 2, 2016 and formally adopted by the European Commission implementing decision C(2016) 4176 final of July 12, 2016.

(f) "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.

(g) "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:

(i) All government-issued identification numbers (including US Social Security numbers, EU Social Security numbers, Canadian Social Insurance numbers, Japanese My Number Social Security/Tax numbers, driver's license numbers, and passport numbers);
(ii) All financial account numbers (bank account numbers, credit card numbers, and other information if that information would permit access to a financial account);
(iii) Individual medical records and biometric information, including any information on any worker or consumer's health, disability, disease or product interests, as well as all data relating to an individual person's health;
(iv) medical, health or genetic information derived from biological samples, such as tissue, blood, urine or other samples, which can directly or indirectly be attributed to an

identified or identifiable individual;
(v) 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;
(vi) Data elements revealing race, ethnicity, national origin, religion, philosophical beliefs, trade union membership, political orientation, sex life or sexual orientation, criminal records, histories of prosecutions or convictions, or allegations of crimes; and
(vii) Any other Personal Information designated by Lilly as Sensitive Personal Information.

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

(i) Any words following the terms 'including,' 'include,' 'in particular' or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.

3. General 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:

(i) 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, or a request from such individual to cease or not begin Processing, or to rectify, block, erase or destroy any such Personal Information;
(ii) 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), or a request from such government official to cease or not begin processing, or to rectify, block, erase or destroy any such Personal Information;
(iii) of any inquiry, claim or complaint regarding the Processing of the Personal Information received by Vendor;
(iv) 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 or a request to cease or not begin processing, or to rectify, block, erase or destroy any such Personal Information.

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. 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 to, or permit remote access to the Personal Information by, 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. Vendor agrees to execute and undertake such compliance mechanisms as may be required by Applicable Laws that apply to Lilly or its affiliates (including data protection laws in any of the members of the European Economic Area ("EEA") and Switzerland) in order for Vendor to receive Personal Information from or send Personal Information to such countries.

Without prejudice to the above, before Vendor receives Personal Information directly from a member state of the EEA or Switzerland in a country that is not deemed to provide an adequate level of data protection by the EU Commission, Vendor must:

(i) promptly cooperate with Lilly or its affiliates to duly complete, execute and comply with the Standard Contractual Clauses as provided by the EU Commission (set forth on Lilly's Procurement Portal as "EU Standard Contractual Clauses for Data Transfer") with respect to all transfers of or remote access to Personal Information from the EEA and/or Switzerland to or by Vendor, as the case may be; or

(ii) notwithstanding the above, in the event that Vendor receives Personal Information from a member state of the EEA or Switzerland in the USA and Vendor is certified under a Data Transfer Program, Vendor hereby warrants that: (a) the certification in question covers the Services, and the intended Processing of the Personal Information, by Vendor as set forth in the Agreement; (b) Vendor will remain certified under such Data Transfer Program during such time as Vendor Processes the Personal Information; and (c) if at any time during such time as Vendor Processes the Personal Information, Vendor de-certifies or otherwise loses the certification in question or for some reason the Data Transfer Program becomes invalid, Vendor will comply with subsection (i) above; or

(iii) if the Vendor cannot comply with either subsection (i) or (ii) above for any reason, the Parties shall cooperate to promptly settle on and execute appropriate alternative

compliance measures.

In all cases, each Party shall bear its own costs incurred in relation to such establishing and maintaining such compliance measures. In respect of data transfers from the EEA or Switzerland, Lilly and Vendor may, by mutual written agreement, terminate or modify data transfer agreements or other compliance measures should they become unnecessary following any European Commission positive adequacy decision under Article 25(6) of the Directive being issued in relation to the country in question (or relevant sector thereof), or if the Directive becomes directly applicable in such country, provided that Vendor shall first self-certify or take any other necessary steps as may be necessary to benefit from that adequacy determination.

If Vendor receives Personal Information originating in the EEA or Switzerland from Lilly or its USA affiliated entities that are certified to a Data Transfer Program, Vendor shall Process such Personal Information in a manner consistent with, and providing the same level of protection as, the Data Transfer Programs. If Vendor determines, for whatever reason and acting reasonably, that it can not provide the same level of protection as is required by the Data Transfer Programs, it shall give Lilly immediate written notification of such determination and Vendor shall immediately remediate such Processing or, if it is unable to do so, cease any and all Processing of such Personal Information.

(f) In the event of permitted transfer or access of Personal Information from the Vendor to a third party, Vendor undertakes to do so only by way of a written agreement with the said third party, which imposes the same obligations on the third party as are imposed on the Vendor under this Standard, including those in 3(e).

Any breach of the above provisions 3(e) and/or 3(f) by the Vendor shall be considered a material breach of the Agreement by Vendor and shall allow Lilly to immediately terminate the Agreement between the parties, by law, and if Lilly elects to terminate this Agreement, Lilly shall provide notice to Vendor as set forth in the notice section of the Agreement.

(g) 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.

(h) 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 Agreement by Lilly, including information required to access Lilly systems or facilities, the maintenance of individual performance metrics and similar information.

(i) Notwithstanding anything in this Agreement to the contrary: (a) No action by Lilly expressly permitted by the Vendor Privacy Standard is a breach of this Agreement by Lilly, and (b) no such action excuses Vendor's performance under this Agreement.

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 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 as required by this Standard and the Agreement 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 or in a computer system under Vendor's control, the Vendor shall comply with following specific standards:

(i) Access Rights: Vendor shall have an effective process to administer access rights. The process shall include the following controls: 1. users and system resources shall only be given the access necessary to perform their required functions; 2. access rights shall be updated based on personnel or system changes; and 3. 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.

(ii) Access Procedures: Vendor shall:

1. 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. 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; and
3. 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.

(iii) 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.

(iv) 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.

(v) Other Controls: Vendor shall:

1. ensure that systems are developed, acquired, and maintained with appropriate security controls.
2. identify systems and applications that warrant security event monitoring and logging, and reasonably maintain and analyze log files.
3. 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. 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. maintain reasonable and appropriate insurance coverage in relation to the risks associated with the Processing.
6. ensure that Personal Information collected for different purposes will be processed separately. In particular, Vendor shall ensure that Personal Information processed on behalf of Lilly and/or its affiliates under this Agreement will be processed separately from other clients' data.

(f) Sensitive Personal Information may not be stored on any portable computer devices or media (including 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 co-operate 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 this Standard, 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) 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 all Applicable Laws.

7. EEA/Switzerland-Specific Terms.

(a) Unless otherwise notified, if Vendor is Processing Personal Information transferred to it (directly or indirectly) from the EEA or Switzerland on the basis of the Standard Contractual Clauses under provision 3(e)(i), Vendor must comply with the obligations imposed on a 'data importer' (or, as applicable, a 'subprocessor') under the Standard Contractual Clauses as provided by the EU Commission (set forth on Lilly's Procurement Portal as "EU Standard Contractual Clauses for Data Transfer") modified as necessary in respect of such Personal Information. Vendor

hereby grants any applicable third party beneficiary rights referred to in the Standard Contractual Clauses.

(b) Where an individual to whom such Personal Information pertains (a "data subject"), or entity acting on his/her behalf, is entitled to bring a claim against Lilly or its affiliate(s) for breach of the Standard Contractual Clauses, and such claim arises from Vendor's processing operations under this Agreement and Standard, Vendor shall indemnify Lilly or its affiliate(s) for all liabilities, costs, expenses, damages and losses (including any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs, calculated on a full indemnity basis, and all other reasonable professional costs and expenses) suffered or incurred by Lilly or its affiliate(s) arising out of or in connection with such claim, provided that:

i. as soon as reasonably practicable, Vendor is given notice of such claim; and
ii. Lilly or its affiliate(s) (as the case may be) shall not make any admission of liability, agreement or compromise in relation to such claim without the prior written consent of Vendor (such consent not to be unreasonably conditioned, withheld or delayed), provided that Lilly or such affiliate(s) may settle such claim (after giving prior written notice of the terms of settlement (to the extent legally possible) to Vendor, but without obtaining Vendor's consent) if Lilly or such affiliate(s) believes that failure to settle such claim would be prejudicial to Lilly or its affiliate(s) in any material respect.

(c) Promptly upon request from Lilly or its affiliates, Vendor shall return to Lilly or a requesting affiliate (if any) a completed Data Processing Information Form using the template set out in Exhibit A.

EXHIBIT A

Vendor Privacy and Security Standard Data Processing Information Form
(to be completed by Vendor and returned to Lilly upon request from Lilly or its affiliates)

Vendor represents that the following is accurate to the best of their knowledge:

1. **Vendor's Registered Name and Address:**

2. **Describe the nature and purpose of the data Processing to be undertaken by Vendor as set forth in the description of Services:**

3. **Select the categories of data of Data Subjects that will be Processed by Vendor as part of the Services:**

   - ☐ Employee Data
   - ☐ Consumer Data
   - ☐ Healthcare Provider Data
   - ☐ Animal Healthcare Provider Data
   - ☐ Clinical Trial Subject Data
   - ☐ Clinical Investigator Data
   - ☐ Vendor and other Contractor Employee Data
   - ☐ Other Personal Information Processed (please list):

4. **Select the categories of data of Lilly that will be Processed by Vendor as part of the services:**

   - ☐ The following data of customers and business partners as well as contact persons at customers and business partners: name, company, location, address(es), contact person, communication data, preferred/excluded communication channels, desired information/ordered newsletters, dispatch, freight, and payment conditions, account advisers, activities, participation in events, campaigns, customer satisfaction, customer-value-score and data of prospective customers.

   - ☐ The following data of health care professionals, including thought leaders: name, institution, location, address(es), contact persons, communication data, CV-data, such as education, areas of expertise, skills and experience, cooperation during clinical trials or observational studies, potential conflicts of interests, participation in events, payment conditions.

   - ☐ The following data of visitors of websites: IP Address, date and time of visit of website, web pages visited, website visitor came from, type of browser visitor is using, type of operating system visitor is using, domain name and address of visitor's

internet service provider, and, as the case may be, data manually entered by the visitor.

- ☐ The following data of employees of Lilly (staff, freelancers, managing directors, and members of the executive board): in particular personnel master data, e.g. data derived from CVs, salary accounting data, data in relation to trainings and performance management, data in relation to company pension schemes, vacation times, absent times, travel expenses, data in relation to driver's licenses, accidents at work, system log data, as well as all data potentially collected in the personnel records.

- ☐ The following data of patients: patient master data, including data in relation to state of health, medication, information in relation to patient support programs, information in relation to the notification of adverse events and product complaints, etc.

- ☐ Business communication with contact persons, in particular: traffic data of e-mail, facsimile, telephone and content of emails, facsimile, and postal communication.

- ☐ Data and results deriving from surveys and other market research activities; accounts and sub-accounts (e.g. contact data, contact person/s, activities, dispatch, freight, and payment conditions), person in charge at Processor.

- ☐ Contract master data, offers, prices, special conditions, order and delivery data, invoice data, payment data, bank account data, data in relation to outstanding payments, and in each case the history relating thereto.

- ☐ Business documents and text as well as the related history with respect to individual business partners, customers, potential customers and business partners, contacts, accounts or other data records that are stored in the system.

- ☐ Data accrued within the scope of use of services that are provided by Lilly (e.g. personnel identification derived from input and usage trails).

5. **Vendor will Process the Personal Information in the following geographies (list countries where Processing operations will occur):**