CVS PHARMACY, INC
DATA PRIVACY AND SECURITY REQUIREMENTS
STANDARD CONTRACT EXHIBIT

This **Exhibit B** ("Exhibit"), is hereby incorporated by reference into the _____ **Agreement** by and between [**CVS Pharmacy, Inc.][Caremark LLC][Correct CVS Caremark Entity]** (herein "CVS") and _____ (herein the "Vendor"), with an effective date of _____ (the "Agreement"). Capitalized terms used in this Exhibit have the meaning assigned in the Agreement unless otherwise defined herein. The terms of this Exhibit supersede any conflicting terms of the Agreement.

Vendor agrees that it shall comply with the following provisions with respect to all CVS Information Assets collected, used, transmitted or maintained for CVS and its affiliates. This Addendum stipulates privacy, confidentiality, and security requirements (including those requirements for Vendor to maintain compliance with the CVS Caremark Vendor Assessment Program (VAP) and demonstrates compliance with applicable privacy, security and data protection laws.

1. Definitions.

1.1. "CVS Information Assets" mean information or data created, collected, generated, licensed, leased, or purchased by or on behalf of CVS or its subsidiaries or information or data otherwise under the control or responsibility of CVS or its subsidiaries, wherever located, including, but not limited to, Personal Information, Intellectual Property, and Financial Records, that are disclosed pursuant to or as part of the Agreement by CVS to Vendor.

1.2. "Financial Records" means all records relating to the finances of the company; stock and debt instruments; accounts and records showing the receipt, management, and disbursement of funds; accounts payable and accounts receivable information; purchase and travel card information; travel and expense information; credit card and merchant account information; and other similar data, including, but are not limited to, receipts, records, minutes of meetings in which financial decisions are made, bank statements, expense vouchers, cancelled checks, debit memoranda, and receipts.

1.3. "Intellectual Property" means any information or CVS property in the form of patents, trademarks, service marks, trade names, trade secrets, and copyrights. This definition incorporates without limitation, technology, designs, processes, machines, manufacture, composition of matter, know-how, computer programs, product designs, market and business plans, all registered and unregistered designs, copyrightable works (including rights in software, firmware, and hardware), design rights, database rights, domain names, rights in confidential information and all similar property rights anywhere in the world in each case whether registered or not and including any application for registration of the foregoing.

1.4. "Personal Information" means any and all information or data (regardless of format) that (i) identifies or can be used to identify, contact or locate an individual, or (ii) that relates to an individual, whose identity can be either directly or indirectly inferred, including any information that is linked or linkable to that individual regardless of the citizenship, age, or other status of the individual.

1.5. "Processing" or "Process" means any operation or set of operations which is performed upon CVS Information Assets, whether or not by automatic means, such as access, collection, compilation, use, disclosure, duplication, organization, storage, alteration, transmission, combination, redaction, erasure, or destruction.

1.6. "Protected Health Information" shall have the same meaning as the term 'Protected Health Information" in 45 CFR § 160.103.

1.7. "Sensitive Personal Information" is a subset of Personal Information, which due to its nature has been classified by law or by CVS policy as deserving additional privacy and

security protections. Sensitive Personal Information consists of: (i) all government-issued identification numbers, (ii) all financial account numbers (including payment card information and cardholder data, as defined by the Payment Card Industry Data Security Standard ("PCI DSS"), (iii) individual medical records (including Protected Health Information, as defined above) and biometric information, (iv) all data obtained from a consumer reporting agency (such as employee background investigation reports, credit reports, and credit scores), (v) data elements revealing race, ethnicity, national origin, religion, trade union membership, sex life or sexual orientation, and criminal records or allegations of crimes, and (vi) any other Personal Information designated by CVS as Sensitive Personal Information.

1.8. "Services" means any and all services that CVS requests the Vendor to perform under the Agreement that involves Processing of CVS Information Assets.

2. Privacy and Data Protection Obligations.

2.1. Vendor shall Process CVS Information Assets only as authorized and as necessary to perform the Services. The Parties agree that CVS will be and remain the owner and controller of the Personal Information for purposes of all applicable privacy laws with rights under such laws to determine the purposes for which the Personal Information is Processed, and nothing in this Agreement will restrict or limit in any way CVS's rights or obligations as owner and/or controller of the Personal Information for such purposes. As such, CVS is directing Vendor to Process the Personal Information in accordance with the terms of this Agreement. The Parties also acknowledge and agree that Vendor may have certain responsibilities prescribed as of the Effective Date by applicable privacy laws as a processor of Personal Information, and Vendor hereby acknowledges such responsibilities to the extent required thereby for processors of personal data.

2.2. Vendor shall immediately inform CVS in writing: (i) if it cannot comply with any material term of the Agreement regarding the Services (if this occurs, Vendor shall use reasonable efforts to remedy the non-compliance, and CVS shall be entitled to terminate any of Vendor's further Processing of CVS Information Assets, in accordance with the provisions contained in the Agreement); (ii) of any request for access to any Personal Information received from an individual who is (or claims to be) the subject of the data; or, (iii) of any request for access to any CVS Information Assets received by Vendor from any government official (including any data protection agency or law enforcement agency) or from 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 CVS or the response is legally required under a subpoena or similar legal document issued by a government agency that compels disclosure by Vendor.

2.3. If the Services involve the collection of Personal Information directly from individuals, Vendor will provide the individuals with a clear and conspicuous privacy notice.

2.4. Vendor shall not transfer Personal Information outside of the United States or, when such is approved by the CVS, across any national borders or permit access to the Personal Information by any employee, affiliate, contractor, or other third party outside of the United States or, when such is approved by the CVS, the country in which the Personal Information is located unless Vendor has the prior written consent of CVS for each such transfer or access. If any country where Services are to be rendered under the Agreement has or enacts a data protection-related law that CVS concludes, in its sole judgment, requires the execution of a supplemental agreement ("Data Processor Agreement") that provides for data protection surrounding the Processing of Personal Information, then Vendor shall, upon CVS's request, execute and cause any Subcontractor to execute such

supplemental agreement prior to further Processing of Personal Information, including any related transfer or access, in such country.

2.5. In the event that the Vendor would be required under the Agreement to Process Personal Information that constitutes Protected Health Information, Vendor will execute a Business Associate Agreement ("BAA") as between the Vendor and CVS prior to any use, access, or disclosure of Protected Health Information. If any provisions of this Exhibit are contrary to those of the BAA, such that it is impossible to comply with both, the more stringent provision shall apply. For purposes of this section, the terms "contrary" and "more stringent" shall have the same meaning as such terms as used in 45 CFR § 160.202, substituting the BAA and this Exhibit for state law and the Privacy Rule respectively, in such definitions.

2.6. The Parties agree, notwithstanding any other provisions of this Agreement to the contrary, that the other Party and their respective Affiliates may store, access and otherwise process their own and each other's business contact information (i.e., the names, business phone, and facsimile numbers, business office and email addresses) of their own and each other's employees anywhere they do business for purposes of this business relationship as it relates to this Agreement and the delivery and/or receipt and use of Services. Each Party may also share such business contact information relating to employees of the other party with contractors, business partners, assignees and others acting on such Party's behalf, but only for use with respect to Services and this Agreement.

2.7. Vendor shall reasonably cooperate with CVS and with CVS's affiliates and representatives in responding to inquiries, claims and complaints regarding the Processing of the Personal Information.

2.8. Vendor shall notify CVS promptly of any request, complaint, claim, or other communication received by the Vendor or Subcontractor from a Data Subject or a Supervisory Authority (as defined below) relating in whole or in part to the Services (each, a "Data Protection Communication"), and shall promptly provide reasonable assistance as requested by CVS in connection with any Data Protection Communication. "Supervisory Authority" means a body with regulatory powers applicable to CVS or a CVS Affiliate.

2.9. CVS undertakes for itself and on behalf of each CVS Affiliate to respond to any Data Protection Communication that is notified to CVS under the preceding paragraph, including, but not limited to, a request from a Data Subject for a copy of the documentation specified in the EU Model Clauses.

3. Information Security Obligations.

3.1. Vendor shall have implemented and documented reasonable and appropriate administrative, technical, and physical safeguards to protect CVS Information Assets against accidental or unlawful destruction, alteration, unauthorized or improper disclosure or access. Vendor shall monitor access to, use and disclosure of CVS Information Assets whether in physical or electronic form. Vendor will regularly test and monitor the effectiveness of its safeguards, controls, systems and procedures. Vendor will periodically identify reasonably foreseeable internal and external risks to the security, confidentiality, integrity, and availability of the CVS Information Assets, and ensure that these risks are addressed. Vendor shall use secure user identification and authentication protocols, including, but not limited to unique user identification, use of

appropriate access controls, and strict measures to protect identification and authentication processes.

3.2. Prior to allowing any employee or contractor to Process any Personal Information, Vendor shall (i) conduct an appropriate background investigation of the individual (and receive an acceptable response), (ii) require the individual to execute an enforceable confidentiality agreement (in a form acceptable to the CVS), and (iii) provide the individual with appropriate privacy and security training. Vendor will also monitor its workers for compliance with the security program requirements. Upon request, Vendor shall provide to CVS a list of all individuals who have (or have had) access to the Personal Information.

3.3. If the Processing involves the transmission of Personal Information, 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. If the Personal Information is stored on systems with connections to wireless, insecure, or public networks, Vendor shall encrypt all Personal Information stored on such systems.

3.4. Sensitive Personal Information may not be stored on any portable or mobile devices or media (including, without limitation, laptop computers, removable hard disks, USB or flash drives, personal digital assistants (PDAs) or mobile phones, DVDs, CDs or computer tapes) unless the Sensitive Personal Information is encrypted.

3.5. Upon request, Vendor shall provide CVS with information about the Vendor's information security program. Vendor shall also submit to a review of its security program through the CVS Caremark Vendor Assessment Program ("VAP"), which shall be carried out by CVS (or by an independent inspection company designated by CVS). Vendor shall reasonably co-operate with any review for the VAP. In the event that the review under the VAP reveals material gaps or weaknesses in Vendor's security program, CVS shall be entitled to suspend transmission of CVS Information Assets to Vendor and terminate Vendor's Processing of CVS Information Assets until such issues are resolved.

3.6. Vendor will promptly and thoroughly investigate all allegations, suspicions, and potential and actual discoveries of unauthorized or improper access to, use or disclosure of the CVS Information Assets, especially those involving Personal Information. Vendor will immediately notify CVS upon discovery of any such unauthorized access to, use or disclosure of the CVS Information Assets (a "security breach") and provide such notification before any notification to any government official (including any data protection agency or law enforcement agency). Vendor shall bear all direct costs associated with resolving a security breach involving the CVS Information Assets maintained by Vendor, including (i) conducting an investigation including reasonable fees associated with computer forensics work, (ii) reasonable cost of providing notice of the security breach to individuals affected by the security breach, and (iii) reasonable cost of providing notice to government agencies, credit bureaus, and/or other required entities (including media notifications), (iv) providing individuals affected by the security breach with credit protection services designed to prevent fraud associated with identity theft crimes for a specific period not less than twelve (12) months, but at least as long as applicable law specifies, (v) reasonable call center support for such affected individuals for a specific period not less than ninety (90) calendar days, but at least as long as applicable law specifies, (vi) non-appealable fines or penalties assessed by

governments or regulators, and (vii) reasonable costs or fees associated with any obligations imposed by applicable law in addition to the costs and fees defined herein.

3.7. When the Vendor ceases to perform Services for CVS, Vendor will either (i) return CVS Information Assets (and all media containing copies of the CVS Information Assets) to CVS, or (ii) purge, delete and destroy the CVS Information Assets. Electronic media containing CVS Information Assets will be disposed of in a manner that renders the CVS Information Assets unrecoverable. Upon request, Vendor will provide CVS with an Officer's Certificate to certify its compliance with this provision.

3.8. Vendor shall carry appropriate insurance to address the risks from its Processing of the CVS Information Assets. CVS shall be named a third party beneficiary of these policies.

4. Use and Disclosure Limitations.

4.1. CVS Information Assets consisting of Personal Information are considered Confidential Information of CVS and Vendor must maintain all such CVS Information Assets in strict confidence. Vendor may disclose CVS Information Assets to its employees and workers, but only to the extent such individuals have a current purpose and need to access to and use of the CVS Information Assets to perform the Services.

4.2. Vendor shall not disclose, transmit, or otherwise make CVS Information Assets available to other third parties (including subcontractors) unless such Processing is required to perform the Services or has been explicitly authorized by CVS in writing. Vendor agrees to contract with any third parties that will handle CVS Information Assets using the terms as found in this Agreement. Any rights that CVS may exercise in connection with this Exhibit in relation to Vendor, Vendor will ensure CVS may also exercise in relation to any such third party.

5. Other Requirements.

5.1. Vendor's Processing shall comply with all applicable privacy or security laws and regulations

5.2. Vendor shall abide, the extent applicable, with Vendor's own privacy notices.

5.3. Vendor certifies that it is now and shall remain in compliance with all applicable state laws in the United States, including (without limitation) Massachusetts 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth and similar state statutes.

CVS Pharmacy, Inc.	Vendor
By:_____	By:_____
Name:_____	Name:_____
Title:_____	Title:_____
Date:_____	Date:_____