Addendum B

Beacon Hill Staffing Group Personnel Covenants

Reference is made to that certain Vendor Agreement between Entellects Corp DBA Beedata Technologies Inc ("Contractor") and Beacon Hill Staffing Group, LLC ("Beacon Hill") dated on or about January 27, 2025 (the "Exhibit A Purchase Order"). Pursuant to the Exhibit A, Contractor agreed to provide certain services to Beacon Hill's "Client" who has engaged Beacon Hill for staffing services. Beacon Hill and its Client, CVS Pharmacy, Inc., have entered into certain Professional Services Agreement dated as of August 1, 2018 (the "CVS Agreement"). Pursuant to the CVS Agreement, CVS has required that Beacon Hill's contractor and its employees agree to certain flowdown provisions contained in the CVS Agreement, as set forth below. Therefore, in consideration of its continued employment by Contractor and Contractor's continued engagement by Beacon Hill and other valuable consideration, the undersigned Contractor employee agrees as follows:

1. Contractor employee agrees to be bound by the privacy and security requirements in Section 6.2 of the CVS Agreement, specifically the Data Privacy Addendum and the Security Addendum attached hereto.

2. Contractor employee agrees to be bound by the firewall requirements in Section 6.5 of the CVS Agreement, a copy of which are attached hereto.

3. Contractor employee agrees to be bound by the "Prohibited Services" provision of Exhibit A of the CVS Agreement, a copy of which is attached hereto.

Signature: *Rachina Chinta*

Contractor Name: Rachina Chinta Rachina Chinta

Date: 2025-01-15

Signature Certificate

Document name:
Rachina Chinta - CVS Addendum

Unique document ID:
a5b2b2f4-a6cd-4a52-9634-13f059ea5f2e

Document fingerprint:
a6926a9f921c2e9c3879b1d08b11a68349de7710214307e6933814e270591ca7ff16202dbaf2557a45815
0f452389cfe922e2e0057e81b65f84b47bed96b664e

Signatories

Rachina Chinta Email: rachinachinta38@gmail.com Device: Chrome 131.0.0.0 on Unknown Windows 10.0 (desktop) IP number: 24.14.161.255	Trusted timestamp: 2025-01-15 19:49:24 UTC *Rachina Chinta*
Michael Cummins **Beacon Hill Staffing** Email: mcummins@beaconhillstaffing.com Device: Chrome 131.0.0.0 on Unknown Windows 10.0 (desktop) IP number:	Verified with login Trusted timestamp: 2025-01-15 19:44:49 UTC *Michael Cummins*

This document was completed by all parties on:

2025-01-15 19:49:24 UTC

GetAccept

Audit log

Trusted timestamp	Event with collected audit data
2025-01-15 19:49:24 UTC	Document was signed by Rachina Chinta (rachinachinta38@gmail.com) Device: Chrome 131.0.0.0 on Unknown Windows 10.0 (computer) IP number: 24.14.161.255 - IP Location: Westmont, United States
2025-01-15 19:49:15 UTC	Document was verified via handwritten signature by Rachina Chinta (rachinachinta38@gmail.com) Device: Chrome 131.0.0.0 on Unknown Windows 10.0 (computer) IP number: 24.14.161.255 - IP Location: Westmont, United States
2025-01-15 19:48:48 UTC	Document was opened by Rachina Chinta (rachinachinta38@gmail.com) Device: Chrome 131.0.0.0 on Unknown Windows 10.0 (computer) IP number: 24.14.161.255 - IP Location: Westmont, United States
2025-01-15 19:44:58 UTC	Document was sent to Rachina Chinta (rachinachinta38@gmail.com) Device: Chrome 131.0.0.0 on Unknown Windows 10.0 (computer) IP number: 96.95.65.177 - IP Location: Oak Park, United States
2025-01-15 19:44:53 UTC	Document was sealed by Michael Cummins (mcummins@beaconhillstaffing.com) Device: Chrome 131.0.0.0 on Unknown Windows 10.0 (computer) IP number: 96.95.65.177 - IP Location: Oak Park, United States
2025-01-15 19:44:49 UTC	Document was signed by Michael Cummins (mcummins@beaconhillstaffing.com) Device: Chrome 131.0.0.0 on Unknown Windows 10.0 (computer)
2025-01-15 19:44:48 UTC	Document was verified via handwritten signature by Michael Cummins (mcummins@beaconhillstaffing.com) Device: Chrome 131.0.0.0 on Unknown Windows 10.0 (computer)
2025-01-15 19:42:42 UTC	Document was created by Michael Cummins (mcummins@beaconhillstaffing.com) Device: Chrome 131.0.0.0 on Unknown Windows 10.0 (computer) IP number: 96.95.65.177 - IP Location: Oak Park, United States

BEACON HILL STAFFING GROUP

BUSINESS STATUS CERTIFICATION

Section 1

Please mark (X) to identify applicable certifications of you Company:

x Minority-Owned Business Enterprise (MBE)

Woman-Owned Business Enterprise (WBE)

Small Disadvantaged Business (DBE)

Veteran-Owned Business (VBE)

HUBZone Business

Small Business Enterprise (SBE)

Other, please specify

None of these apply

Section 2

Please provide company DUNS #: 55-623-7621

Section 3

If you indicated in **Section 1** that your company is certified please provide the following information regarding your certification, along with a **copy of Certificate** with this form:

Agency

Certification number

Expiration date

****

In accordance with FAR 52.219-1 and under 15 USC 645(d) any person who misrepresents a firms *SBIHUBZone/SDB/WOSB* status in order to obtain a contract or subcontract shall be punishable by:

(1) A fine, imprisonment or both
(2) Administrative remedies including suspension and debarment
(3) The firm making the misrepresentation shall be ineligible for participation in programs conducted under the authority of the Small Business Act.

Company Entellects Corp DBA Beedata Technologies Inc

Address 6110 McFarland station DR, STE#103, Rolling Meadows, georgia 30005, United States

Signature krishna k

Title Director

Date 1/15/2025

EXHIBIT A

PURCHASE ORDER

In accordance with the Contractor Agreement signed between the undersigned parties on August 21, 2020, it is agreed as follows:

1. Contractor, Entellects Corp DBA Beedata Technologies Inc, with Federal I.D. Number 813460542 and office address at 6110 McFarland station DR, STE#103, Rolling Meadows, georgia 30005, United States, and phone number 6789926388, is contracted to perform work for CVS Health ("Client") beginning January 27, 2025 and terminating January 23, 2026 ----("End Date") at a rate of $60.00 per hour ("Contractor's Rate") to complete work on the following project: Enterprise Finance SAP Lead.

2. Unless otherwise notified, when the End Date has elapsed Contractor shall assume that this Purchase Order has been extended beyond such "End Date" on a month-to-month basis, on the same terms and conditions stated herein and in the Contractor Agreement referenced above, until such time as the above-mentioned project is completed or Contractor provides 30 days prior written notice of a refusal to extend this Purchase Order. For purposes of this Purchase Order, "month-to-month" means the period beginning on the next calendar date immediately after the previous "End Date" and terminating on the same calendar date of the next month (or, if there is not such date, the closest date thereto in that month), which is the new "End Date." Contractor's 30 day written notice shall commence on the actual calendar date that it is received and 30 days thereafter shall be the new "end date."

2a. Unless otherwise notified, when the estimated total amount of the Purchase Order has been exceeded, Contractor shall assume that the Purchase Order has been extended beyond the "total amount" as described in paragraph 1.

3. At the end of each week Contractor shall submit an invoice along with a time sheet provided by BEACON HILL and signed by an authorized official of the Client.

4. Contractor will discuss its hours and location where work is to be performed with the Client, including notification to the Client if Contractor cannot be present.

5. Contractor agrees to complete the assignment within the guidelines as provided by the Client or within any reasonable changes in the guidelines provided by the Client.

6. Contractor's rate is a confidential matter between Contractor and BEACON HILL and shall not be divulged to any other party, including the Client.

7. Client Right to Hire Contractor Personnel. Client is permitted to hire directly Contractor Personnel named on this Exhibit A at any time. Neither Client nor Beacon Hill shall be obligated to pay any hiring, liquidation, or other fee associated with such Client hiring of Contractor Personnel named on this Exhibit A. Contractor agrees to waive, and shall be deemed to have waived, any restrictive covenants then in place with respect to such Contractor Personnel.

8. Client Requirements. As specifically called for in an executed addendum, Contractor agrees that the terms and conditions set forth in this Exhibit A, together with the terms and conditions in any Beacon Hill Client Agreement ("Prime Contract") shall be binding on Contractor as they relate to the Contractor Personnel to be provided by Contractor for the role for which such Contractor Personnel is provided. Contractor agrees to abide by the terms and conditions contained within the following:

- Exhibit B – Client Flow Down (CVS Health), attached hereto

9. The following personnel of Contractor who will work on this project have been informed and understand their obligations under this Purchase Order and the Contractor Agreement:

Name: Rachina Chinta Date: January 27, 2025

10. The undersigned has/have read, understand(s), and agree(s) to the terms and conditions herein.

Entellects Corp DBA Beedata Technologies Inc	BEACON HILL STAFFING GROUP, LLC
Signature: krishna k	Signature:
Name: krishna k Title: Director	Name: Title:
Date: 1/15/2025	Date:

Exhibit B

Client Flow Down (CVS Health)

ADDENDUM TO THE CONTRACTOR AGREEMENT

This Addendum to the Contractor Agreement (hereinafter this "Addendum") is entered into this January 14, 2025, by and between Beacon Hill Staffing Group, LLC. ("Beacon Hill"), and Entellects Corp DBA Beedata Technologies Inc ("Contractor"). Both Beacon Hill and Contractor shall be collectively referred to as the "Parties."

WHEREAS, the Parties previously entered into a Contractor Agreement dated August 21, 2020 ("Existing Agreement"). "Agreement" shall collectively refer to this Addendum and the Existing Agreement;

WHEREAS, the Parties wish to amend the Existing Agreement and add the following for services Contractor is to perform for CVS Health ("CVS Health" or "Company");

Pursuant to the Existing Agreement, Contractor agreed and acknowledged that, for any particular engagement, certain customer requirements would be flowed down to Contractor. This Agreement sets forth the terms and conditions which are to be flowed to Contractor for all work performed in respect of Beacon Hill's contract with Company. These terms and conditions shall apply to all work performed by Contractor under the applicable Exhibit A (PO) on the Customer project, and to the extent of a conflict, supersede the terms of the Existing Agreement.

THEREFORE, the parties have agreed to amend and restate the Existing Agreement in its entirety and agree that this Addendum shall be deemed to be included in the Existing Agreement and that no other changes are authorized under this Addendum; all other terms and conditions of the Existing Agreement remain unchanged.

BEACON HILL STAFFING GROUP, LLC	Entellects Corp DBA Beedata Technologies Inc
Signature:	Signature: krishna k
Name:	Name: krishna k
Title:	Title: Director
Date:	Date: 1/15/2025

Addendum A

Beacon Hill Staffing Group Personnel Covenants - Vendor

Reference is made to that certain Contractor Agreement between Entellects Corp DBA Beedata Technologies Inc ("Contractor") and Beacon Hill Staffing Group, LLC ("Beacon Hill") dated on or about August 21, 2020 (the "Contractor Agreement"). Pursuant to the Contractor Agreement, Contractor agreed to provide certain services to Beacon Hill's "Clients" who have engaged Beacon Hill for staffing services. Beacon Hill and its Client, CVS Pharmacy, Inc., have entered into certain Professional Services Agreement dated as of August 1, 2018 (the "CVS Agreement"). Pursuant to the CVS Agreement, CVS has required that Beacon Hill's contractor agree to certain flow down provisions contained in the CVS Agreement, as set forth below. Therefore, in consideration of its continued engagement by Beacon Hill and other valuable consideration, the undersigned Contractor agrees as follows:

1. Contractor agrees to be bound by the privacy and security requirements in Section 6.2 of the CVS Agreement, specifically the Data Privacy Addendum and the Security Addendum attached hereto.

2. Contractor agrees to be bound by the requirements defined in the Business Associate Agreement set forth in Section 6.4 of the CVS Agreement, a copy of which is attached hereto.

3. Contractor agrees to be bound by the firewall requirements in Section 6.5 of the CVS Agreement, a copy of which are attached hereto.

4. Contractor agrees to be bound by the "Prohibited Services" provision of Exhibit A of the CVS Agreement, a copy of which is attached hereto.

Entellects Corp DBA Beedata Technologies Inc

Signature: krishna k

Name: krishna k

Title: Director

Date: 1/15/2025

CVS FLOW DOWN PROVISIONS

6.2 Privacy and Security Requirements

Vendor agrees and acknowledges that it is bound by the requirements defined in the Data Privacy and Security Addendum exhibits (the "Privacy Exhibits") that are attached to the Agreement as Exhibit C and Exhibit D and are incorporated herein by reference.

6.4 Business Associate Agreement

Vendor agrees and acknowledges that it is bound by the requirements defined in the Business Associates Agreement ("BAA") between the parties with an effective date of August 1, 2018.

6.5 Firewall

Vendor acknowledges that CVS must maintain a firewall between the CVS retail pharmacy business (the "Retail Business") and the Caremark pharmacy benefits management business (the "PBM Business") to separate certain competitively sensitive information that each business possesses. Vendor agrees that, (1) Vendor will not knowingly transfer competitively sensitive information of the Retail Business to the PBM Business or allow the PBM Business to access such information, and (2) Vendor will not knowingly transfer competitively sensitive information of the PBM Business to the Retail Business or allow the Retail Business to access such Information.

SCOPE OF SERVICES

Vendor is authorized to provide any of the following Services to CVS. Actual Services to be provided will be detailed in a SOW agreed to and signed by the parties.

Authorized Services Provided: Enterprise Staff Augmentation Services.

Authorized CVS Business Areas/Departments: Enterprise.

Authorized CVS Information:
Confidential Information: Protected Health Information; Personal Information.

Prohibited Services
Notwithstanding anything to the contrary in herein, in the Agreement, or any bid package or SOW under the Agreement, Services that may involve Vendor's access to or materials containing Medicare Part D Information as defined in the Agreement, Nondisclosure Agreement, Business Associates Agreement, or Data Privacy and Security Requirements Exhibit, are not authorized under the Agreement. In the event Vendor receives access to said prohibited classes of information, even if such receipt is in error, Vendor shall immediately notify CVS upon discovery, shall be responsible for the security, confidentiality and protection of such information while in Vendor's possession, and shall return all relevant materials immediately as instructed by CVS.

THE AUTHORIZED SERVICES LISTED ABOVE ARE THE ONLY SERVICES AUTHORIZED BY THIS AGREEMENT. ANY ADDITIONAL SERVICES NOT LISTED AS AUTHORIZED SERVICES ABOVE, QUALIFYING AS PROHIBITED SERVICES OR OTHERWISE INVOLVING THE TYPES OF MEDICARE PART D INFORMATION AS DEFINED IN THE PRECEDING PARAGRAPH MUST BE AGREED TO BY BOTH PARTIES IN WRITING THROUGH AN AMENDMENT OF THIS AGREEMENT OR BY ENTERING INTO A SEPARATE AGREEMENT.

DATA PRIVACY ADDENDUM

This Data Privacy Addendum ("Data Addendum"), is hereby incorporated by reference into the Professional Services Agreement by and between CVS Pharmacy, Inc., a Rhode Island corporation, on behalf of itself and on behalf of its subsidiaries and Affiliates including without limitation Caremark Rx, L.L.C., (hereinafter called "CVS") and Vendor Name (herein the "Vendor"), with an effective date of August 1, 2018 (the "Agreement"). This Data Addendum is effective as the effective date of the Agreement ("the Effective Date"). Capitalized terms used in this Data Addendum have the meaning assigned in the Agreement unless otherwise defined herein. The terms of this Data Addendum supersede any conflicting terms of the Agreement.

Vendor agrees that it shall comply with the following provisions with respect to all Personal Information collected, used, transmitted or maintained for CVS and its affiliates. This Data Addendum stipulates privacy and confidentiality requirements.

1. Definitions.

1.1 "Applicable Law" shall mean any all national, state, regional and/or local laws, rules, regulations, security requirements and regulatory guidance applicable to either party's performance under the Agreement including but not limited to those applicable to the Processing of Personal Information.

1.2 "Incident" shall mean the use, disclosure or Processing of Personal Information in any form that is not authorized by this Data Addendum, or the interference with information systems containing Personal Information.

1.3 "Personal Information" has the meaning given by Applicable Law and includes any and all information or data (regardless of format and whether alone or in combination) that relates to an identified or identifiable individual; and is supplied to or Processed by or on behalf of Vendor in connection with the provision of the Services or otherwise for or on behalf of CVS Personal Information.

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

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

1.6 "Services" means any and all services that Vendor is required to perform under the Agreement that involves Processing of Personal Information.

2. Privacy Obligations.

2.1 Vendor shall Process Personal Information only as authorized and as necessary to perform the Services.

2.2 Vendor may disclose Personal Information to its employees and contractors, but only to the extent such individuals have a current purpose and need to access to and use of the Personal Information to perform the Services.

2.3 Vendor shall not disclose, transmit, or otherwise make Personal Information available to other third parties (including subcontractors) unless such Processing is explicitly required to perform the Services or has been explicitly authorized by CVS in writing.

2.4 Vendor agrees to ensure that any agent or subcontractor that may have access to Personal Information has agreed in writing to the same restrictions, conditions and requirements that apply through this Data Addendum to Vendor with respect to such information prior to obtaining such access. Vendor shall be liable to CVS for any acts, failures or omissions of such agents or subcontractor in violation of the requirements of this Data Addendum as if they were Vendor's own acts, failures or omissions, to the extent permitted by law, and any rights that CVS may exercise in connection with this Data Addendum in relation to Vendor, Vendor will ensure CVS may also exercise in relation to any such agent or subcontractor.

2.5 Vendor shall inform CVS in writing within five (5) business days of receipt of any request for access to any Personal Information or

complaint received (i) from or on behalf of an individual who is the subject of the data; (ii) from any government official or agency (including any law enforcement agency) or (iii) from any other third party, other than requests that are required to be responded to as part of the Services as described 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.

2.6 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 Data Addendum are contrary to those of the BAA such that it is impossible to comply with both, the more stringent, protective or restrictive provision shall apply.

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 agrees to report any Incident to CVS immediately, but in no event later than within two (2) business days, after it is discovered. An Incident shall be treated as discovered when any employee, director, officer, or agent of Vendor knows or should have known of such Incident by exercising reasonable diligence. The report shall be made by email to privacy.officer@cvshealth.com and shall contain the following information concerning the Incident: (i) a brief description of what happened, including the date of the Incident and the date of the discovery of the Incident, if known; (ii) the individuals affected; (iii) a description of the data elements involved in the Incident; (iv) any steps individuals should take to protect themselves from potential harm resulting from the Incident; (iv) a brief description of what Vendor is doing to investigate the Incident, to mitigate harm to individuals, and to protect against any further incidents; and (v) any other information reasonably requested by CVS. If such information is not available to Vendor at the time the Incident is required to be reported to CVS, Vendor shall continue to diligently investigate the Incident an provide such information to CVS promptly as it becomes available. The Vendor shall maintain complete records regarding the Incident for a minimum period of six (6) years or such longer period required by applicable law, and shall make such records available to CVS promptly upon request, but in no event later than within forty-eight (48) hours of such request.

3. Remediation and Mitigation

3.1 In the event of an Incident involving Personal Information under the control of Vendor or its agents or subcontractors or any person or entity under Vendor's direction or control, Vendor agrees to perform any reasonable mitigation or remediation services requested by CVS. Vendor further agrees to be responsible for all costs and expenses resulting from or related to the Incident, including but not limited to reasonable costs of providing required notices to individuals affected by the Incident, government agencies, credit bureaus, and/or other required entities.

4. Miscellaneous.

4.1 Vendor agrees to take such action as CVS deems necessary to amend this Data Addendum from time to time to comply with the requirements of applicable law. If Vendor disagrees with any such amendment proposed by CVS, it shall so notify CVS in writing no later than fifteen (15) business days after receipt of CVS's notice of the amendment. If the parties are unable to agree on an amendment, CVS may, at its option, terminate the Services Agreement.

4.2 Vendor's Processing shall comply with all applicable privacy laws and regulations, including (without limitation) Massachusetts 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth and similar state statutes.

4.3 Vendor shall, the extent applicable and consistent with the terms of this Data Addendum, abide by Vendor's own privacy notices and privacy policies and procedures.

4.4 Vendor represents that neither it nor its agents or subcontractors will transfer, access or otherwise handle Personal Information outside the United States without the explicit prior written permission of CVS.

4.5 The parties agree that the remedies at law for a violation of the terms of this Data Addendum may be inadequate and that monetary damages resulting from such violation may not be readily measured. Accordingly, in the event of a violation by either party of the terms of this Data Addendum, the other party shall be entitled to immediate injunctive relief. Nothing herein shall prohibit either party from pursuing any other remedies that may be available to either of them for such violation.

4.6 Any Personal Information provided to Vendor, or created, obtained, procured, used or accessed by Vendor in CVS's name or on CVS's behalf, shall, as between the parties to this Agreement, at all times be and remain the sole property of CVS, and Vendor shall not have or obtain any rights therein except the right to use such data for the purposes stated herein.

SECURITY ADDENDUM

A. Vendor agrees to:

(1) Employ essential current industry practice security controls and tools to monitor its information processing systems and log key events such as user activities (including root or administrative access), exceptions, successful and unsuccessful logins, access to audit logs, unauthorized information processing activities, suspicious activities and information security events;

(2) Ensure that neither it nor any of its employees or contractors ("Workforce") will place Protected Health Information or Personal Information on portable computing/storage devices which are not owned by Vendor;

(a) "Protected Health Information" or "PHI" shall have the same meaning as such term is defined in 45 CFR 160.103, but limited to information created, accessed or received for or on behalf of CVS, or in the course of providing services for CVS;

(b) "Personal Information" has the meaning given by Applicable Law and includes any and all information or data (regardless of format and whether alone or in combination) that relates to an identified or identifiable individual; and is supplied to or Processed by or on behalf of Vendor in connection with the provision of the Services or otherwise for or on behalf of CVS;

(3) Ensure that data files containing PHI and/or PII are not saved on public or private computers while accessing corporate e-mail through the Internet;

(4) Secure all electronic PHI and/or PII in motion;

(5) Secure any PHI and/or PII at rest that is placed or stored on portable devices 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);

(6) Secure all electronic PHI and PII at rest, including ensuring that all electronic PHI held at rest shall be rendered unreadable by unauthorized parties using strong encryption technologies;

(7) Dispose of all PHI and/or PII in a Secure manner, including the permanent removal of all PHI and/or PII from such media or devices before making such electronic media or devices available for re-use;

(8) Make log events available for monitoring to CVS or a managed security service provider as designated by CVS;

(9) Regularly back up activity logs to a secure central location, protected against tampering and unauthorized access;

(10) Retain activity logs in accordance with regulatory requirements;

(11) Perform regular, routine log reviews and take necessary actions to protect against unauthorized access or misuse;

(12) Comply with all applicable regulatory requirements related to monitoring and logging activities;

(13) Ensure that the clocks of all relevant information processing systems will be synchronized using an authoritative national or international time source;

(14) Incorporate date and time stamp into log entries;

(15) Employ, monitor, and keep up to date intrusion detection systems and intrusion prevention systems to monitor all network traffic and alert personnel to suspected security events;

(16) Ensure access to Vendor applications accessible over un-trusted or open networks are controlled and restricted by a defined security perimeter;

(17) Appropriate security barriers including entry controls, authentication controls, malicious or hostile software detection are applied. Access to applications is restricted to authorized parties using authorized protocols.

(18) Obtain certification that its information security safeguards meet or exceed a defined industry information security standard and maintain its safeguards in compliance with such certification requirements and obligations;

(19) Provide to CVS, at CVS's request, a list of its Workforce who have (or have had) access to the Protected Health Information and the work location of each such individuals; and

(20) Submit to controls testing by CVS, or at the sole cost of the Vendor a mutually agreed upon third party, and provide evidence at least annually, demonstrating a process for threat & vulnerability management, including:

(a) Regularly scheduled internal and external system, application, and network vulnerability scans;

(b) Results of network and application layer penetration tests

(c) Results of secure application source code scanning and analysis review; and

(d) Vendor agrees to remediate vulnerabilities to the reasonable satisfaction of CVS.

B. Vendor represents that neither it nor its agents or Subcontractors will transfer, access or otherwise handle PHI and/or PII outside the United States without the explicit prior written permission of CVS.

C. Before obtaining access to or receiving any PHI and/or PII from CVS, Vendor shall 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).

(a) Any Vendor representations made during the VAP or Vendor responses provided to questions as part of the VAP are hereby incorporated into the Master Services Agreement and Vendor shall be obligated to comply with and honor such representations as if they were part of the Agreement.

(b) Vendor shall reasonably co-operate with any review for the VAP.

(c) If the review under the VAP identifies material gaps or weaknesses in Vendor's security program or its ability to Secure PHI and/or PII, CVS shall be entitled to suspend Vendor's access to or use of CVS PHI and/or PII until such issues are resolved to the satisfaction of CVS's Chief Privacy Officer and Chief Information Security Officer.

(d) During the term of this Addendum, CVS may periodically, but no more frequently than once every two years, request that Vendor complete a new VAP. If any subsequent annual review under the CVS VAP identifies any material gaps or weaknesses in Vendor's security program or its ability to Secure PHI and/or PII, CVS shall be entitled to suspend Vendor's access to or use of CVS PHI and/or PII until such issues are resolved to the satisfaction of CVS's Chief Privacy Officer and Chief Information Security Officer.

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is effective as of the Effective Date specified below by and between Beacon Hill Staffing Group ("Business Associate") and CVS Pharmacy, Inc. on behalf of itself and its subsidiaries and affiliates ("CVS") for which Business Associate provides services pursuant to one or more service agreements entered into between the parties (collectively "Services Agreement"). CVS and Business Associate mutually agree to the terms of this Agreement in order to comply with the HIPAA Rules as defined below.

This Agreement is effective as of August 1, 2018 or the effective date of the Services Agreement if earlier than the date of this Agreement (the "Effective Date").

1. Definitions

(a) "Applicable Law" shall mean any national, state, regional and/or local laws, rules, regulations, security requirements and regulatory guidance applicable to either party's performance under the Services Agreement including but not limited to those applicable to the Processing of Personal Information.

(b) "Breach" shall have the same meaning as the term "Breach" in 45 CFR 164.402.

(c) "HIPAA Rules" shall mean the Health Insurance Portability and Accountability Act of 1996, as amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5) (the "HITECH Act") and the federal regulations published at 45 CFR parts 160 and 164 and any other applicable federal and state privacy and security laws regarding individually identifiable health information.

(d) "Individual" shall have the same meaning as such term as defined in 45 CFR 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g) or other applicable federal or state law.

(e) "Incident" shall mean the use, disclosure or processing of Personal Information that is not authorized by this Ag

(f) "Personal Information" has the meaning given by Applicable Law and includes any and all information or data (regardless of format and whether alone or in combination) that relates to an identified or identifiable individual, and is supplied to or Processed by or on behalf of Business Associate in connection with the provision of the Services or otherwise for or on behalf of CVS. Personal Information includes Protected Health Information.

(g) "Process" means any operation which is performed upon Personal Information, whether or not by automatic means, including but not limited to the access, granting access to, acquisition, collection, recording, organization, storage, alteration, retrieval, consultation, use, disclosure, combination, transfer, blocking, return or destruction of Personal Information. "Processed" or "Processing" shall be construed accordingly.

(h) "Protected Health Information" shall have the same meaning as such term is defined in 45 CFR 160.103, but limited to information created, accessed or received for or on behalf of CVS, or in the course of providing services for CVS.

(i) "Satisfactory Background Screening" shall mean, collectively (1) a national federal criminal database check; (2) a seven-year county of residence criminal conviction search; and (3) in each of (1) and (2) above, a screening result which contains no felony or misdemeanor conviction that related to fraud or theft (including but not limited to, shoplifting, larceny, embezzlement, forgery, credit card fraud, or check fraud), the disposition of which is within seven years, as allowed by law.

(j) "Secure" shall mean to render unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of the HITECH Act, as updated from time to time ("Guidance") which, in the case of electronic information, requires that it be encrypted in accordance with standards specified in such Guidance.

All capitalized terms used in this Agreement and not defined elsewhere herein or in the Services Agreement shall have the same meaning as those terms are used or defined in the HIPAA Rules.

2. Obligations of Business Associate with respect to Use and Disclosure of Protected Health Information

(a) Business Associate shall not use or disclose Personal Information except as permitted or required by this Agreement or as Required by Law, and only in compliance with Applicable Law.

(b) Business Associate agrees to satisfy and comply with the HIPAA Rules concerning the confidentiality, privacy, and security of Protected Health Information that apply to business associates. To the extent Business Associate carries out any obligations under the Privacy Rule (45 CFR Subpart E of Part 164) for CVS, Business Associate shall comply with the requirements of the Privacy Rule that apply to the performance of such obligations.

(c) Business Associate agrees to mitigate, at its sole expense, any harmful effect(s) resulting from an Incident.

(d) Business Associate agrees to ensure that any agent or Subcontractor that may have access to Personal Information has entered into a written contract with Business Associate that contains the same restrictions, conditions and requirements that apply through this Agreement to Business Associate prior to an agent or Subcontractor obtaining such access. Business Associate agrees that if Business Associate knows of a pattern of activity or practice of an agent or Subcontractor that constitutes a material breach or violation of the agent's or Subcontractor's obligation under such written contract, Business Associate shall take reasonable steps to cure the breach or end the violation, as applicable, and, if such steps are unsuccessful, terminate the contract, if feasible. Business Associate shall be liable to CVS for any acts, failures or omissions of its agent or Subcontractor in violation of the requirements of this Agreement as if they were Business Associate's own acts, failures or omissions, to the extent permitted by law and any rights that CVS may exercise in connection with this Agreement in relation to Business Associate, Business Associate will ensure CVS may also exercise in relation to any such Subcontractors.

(e) Business Associate agrees that it shall request, use and disclose only a Limited Data Set or, if that is not practicable, only the minimum necessary Personal Information to perform or fulfill a specific function required or permitted under this Agreement. Business Associate agrees to comply with any guidance issued by the Secretary regarding minimum necessary.

(f) If Business Associate conducts, in whole or in part, any Transactions electronically on behalf of CVS, Business Associate shall comply with the applicable requirements of 45 CFR 162 and shall require that any agents or Subcontractors that perform, in whole or in part, such electronic Transactions on its behalf, agree in writing to comply with such requirements. Business Associate will not enter into or permit its agents or Subcontractors to enter into any trading partner agreement in connection with the conduct of Transactions on behalf of the CVS that: (i) changes the definition, data condition, or use of a data element or segment in a Standard Transaction; (ii) adds any data element or segment to the maximum defined data set; (iii) uses any code or data element that is marked or "not used" in the Standard Transaction's implementation specification or is not in the Standard Transaction's implementation specification; or (iv) changes the meaning or intent of the Standard Transaction's implementation specification.

Business Associate agrees to report any Incident to CVS immediately, but in no event later than within two (2) business days, after it is discovered. An Incident shall be treated as discovered when any employee, director, officer, or agent of Business Associate knows or should have known of such Incident by exercising reasonable diligence. Such report shall be made by email to privacy.officer@cvscaremark.com. Business Associate shall provide the following information concerning the Incident: (i) a brief description of what happened, including the date of the Incident and the date of the discovery of the Incident, if known; (ii) the individuals affected; (iii) a description of the data elements involved in the Incident; (iv) any steps individuals should take to protect themselves from potential harm resulting from the Incident; (iv) a brief description of what Business Associate is doing to investigate the Incident, to mitigate harm to individuals, and to protect against any further incidents; and (v) any other information reasonably requested by CVS. If such information is not available to Business Associate at the time the Incident is required to be reported to CVS, Business Associate shall continue to diligently investigate the Incident and provide such information to CVS promptly as it becomes available. The Business Associate shall maintain complete records regarding the Incident for the period required by 45 CFR 164.530(j) or such longer period required by state law, and shall make such records available to CVS promptly upon request, but in no event later than within forty-eight (48) hours of such request.

(g) Within five (5) business days of receipt of a request from CVS, Business Associate shall provide to CVS or, at its direction, to an Individual, Protected Health Information relating to that individual held by Business Associate or its agents or Subcontractors in a Designated Record Set in accordance with 45 CFR 164.524. In the event any Individual requests access to his or her Protected Health Information directly from Business Associate, Business Associate shall, within five (5) business days of receipt of such request, forward the request to CVS unless the Privacy Rule requires Business Associate to receive and respond to such requests directly, in which case Business Associate shall respond directly as required by and in accordance with 45 CFR 164.524, and shall send a copy of such response to CVS.

(h) Within five (5) business days of receipt of a request from CVS, Business Associate agrees to make any requested amendment(s) to Protected Health Information held by it or any agent or Subcontractor in a Designated Record Set in accordance with 45 CFR 164.526. In the event any individual requests an amendment to his or her Protected Health Information directly from Business Associate, Business Associate shall, within five (5) business days of receipt thereof, forward such request to CVS.

(i) Within ten (10) business days after Business Associate, its agents or Subcontractors makes any disclosure of Protected Health Information for which an accounting may be required under 45 CFR 164.528, Business Associate agrees to provide in writing via email to privacy.officer@cvscaremark.com, the information related to such disclosure as would be required to respond to a request by an Individual for an accounting in accordance with 45 CFR 164.528. In the event any Individual requests an accounting of disclosures under 45 CFR 164.528(a) directly from Business Associate, Business Associate shall, within ten (10) business days of receipt of such request, forward the request to CVS unless the Privacy Rule requires or CVS directs that Business Associate to receive and respond to such requests directly, in which case Business Associate shall respond directly as required by and in accordance with 45 CFR 164.528, and shall send a copy of such response to CVS.

(j) Within five (5) business days of receipt of a request from CVS, Business Associate agrees to comply with any request for confidential communication of, or restriction on the use or disclosure of, Protected Health Information held by it or any agent or Subcontractor as requested by CVS and in accordance with 45 CFR 164.522.

(k) Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of Personal Information available to the Secretary of Health and Human Services or her/his designees or other government authorities in a time and manner designated by CVS or such governmental authorities, for purposes of determining compliance with Applicable Law. Business Associate shall provide a copy of such books and records to CVS at the same time as these are provided to the Secretary or other government authorities.

(l) Business Associate shall maintain documentation of its obligations hereunder to the extent and for the period required by Applicable Law, including 45 CFR 164.530(j).

(m) Notwithstanding any other provisions of this Agreement, to the extent CVS provides prior written permission for the handling of Personal Information by Business Associate or its agents or Subcontractors outside the United States pursuant to Section 7(f) below, Business Associate agrees to comply with the requirements of the CMS memorandum of July 23, 2007 entitled " Sponsor Activities Performed Outside of the United States (Offshore Subcontracting)" with respect to Protected Health Information of Medicare beneficiaries. The terms specified in the attestation contained in that CMS memorandum are hereby incorporated by reference.

3. Security of Protected Health Information

(a) Business Associate shall have implemented and documented reasonable and appropriate administrative, technical, and physical safeguards to protect Personal Information and Protected Health Information against accidental or unlawful destruction, alteration, unauthorized or improper disclosure, or access. Business Associate shall monitor access to, use and disclosure of Personal Information and Protected Health Information whether in physical or electronic form. Business Associate will periodically identify reasonably foreseeable internal and external risks to the security, confidentiality, integrity, and availability of the Personal Information and Protected Health Information, and ensure that these risks are addressed. Business Associate 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.

(b) To protect against unauthorized access or use of CVS Health Personal Information or Protected Health Information residing on Business Associate Information Processing Systems, Business Associate will:

(i) Employ essential current industry practice security controls and tools to monitor Information Processing Systems and log key events such as user activities (including root or administrative access), exceptions, successful and unsuccessful logins, access to audit logs, unauthorized information processing activities, suspicious activities and information security events;

(ii) Make log events available for monitoring to CVS or a Managed Security Service Provider as designated by CVS

(iii) Regularly back up activity logs to a secure central location, protected against tampering and unauthorized access;

(iv) Retain activity logs in accordance with regulatory requirements;

(v) Perform regular, routine log reviews and take necessary actions to protect against unauthorized access or misuse;

(vi) Comply with all applicable regulatory requirements related to monitoring and logging activities;

(vii) Ensure that the clocks of all relevant information processing systems will be synchronized using an authoritative national or international time source;

(viii) Incorporate date and time stamp into log entries; and

(ix) Employ, monitor, and keep up to date intrusion detection systems and intrusion prevention systems to monitor all network traffic and alert personnel to suspected security events.

(c) Business Associate warrants and represents that Business Associate has obtained, at Business Associate's own expense and in a manner compliant with all applicable local, state, federal and international laws, a Satisfactory Background Screening for all of its employees and contractors with access to any Personal Information or Protected Health Information ("Workforce Members"). Business Associate agrees to update such background screening upon reasonable request by CVS, it being agreed that any request based upon the occurrence of any Incident or illegal activity or reasonable suspicion of illegal activity involving Personal Information by Workforce Members, or any regulatory requirements requiring such updates, shall be deemed reasonable. In addition, prior to allowing any Workforce Members to Process any Personal Information or Protected Health Information, Business Associate shall require the Workforce Member to execute an enforceable confidentiality agreement (in a form acceptable to the CVS), and provide the Workforce Member with appropriate privacy and security training. Business Associate will also monitor its Workforce Members for compliance with the security program requirements. Upon request, Business Associate shall provide to CVS a list of all Workforce Members who have (or have had) access to the Personal Information and the work location of each such Workforce Member.

(d) Business Associate agrees to Secure all electronic Personal Information and Protected Health Information in motion and all electronic Personal Information and Protected Health Information placed or stored on portable devices 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), and to dispose of all Personal Information and Protected Health Information in a Secure manner, including the permanent removal of all Personal Information or Protected Health Information from such media or devices before making such electronic media or devices available for re-use. Notwithstanding the foregoing, beginning January 1, 2016, Business Associate agrees all electronic Personal Information and Protected Health Information held at rest and in transit shall be rendered unreadable by unauthorized parties using strong encryption technologies.

(e) Business Associate shall obtain certification against a defined industry standard and maintain their program in compliance with its requirements and obligations.. Documentation of Business Associate's security assessments, including testing and any remediation efforts must be retained for a period of six (6) years following (i) termination hereof and (ii) destruction or return of Personal Information or Protected Health Information, whichever is last to occur, or such longer period as required by applicable law. Business Associate shall train Workforce members on the responsibilities under this Agreement, including the responsibilities to safeguard and, where appropriate or required, Secure Personal Information or Protected Health Information, and consequences for failing to do so.

(f) Business Associate will submit to controls testing by CVS Health, or at the sole cost of the Business Associate a mutually agreed upon Supplier, and provide evidence at least annually, demonstrating a process for threat & vulnerability management, including:

(i) Regularly scheduled internal and external system, application, and network vulnerability scans;
(ii) Results of network and application layer penetration tests;

(iii) Results of Secure application source code scanning and analysis review; and

(iv) Business Associate agrees to remediate vulnerabilities according a defined framework that is equivalent to the standard established by CVS.

(g) Business Associate agrees that access to applications accessible over untrusted or open networks are controlled and restricted by a defined security perimeter. Appropriate security barriers including entry controls, authentication controls, malicious or hostile software detection are applied. Access to applications is restricted to authorized parties using authorized protocols.

(h) Business Associate agrees that neither it nor any of its Workforce members will place Personal Information or Protected Health Information on portable computing/storage devices that are not owned by Business Associate. Business Associate shall ensure that data files containing

Personal Information or Protected Health Information are not saved on public or private computers while accessing corporate e-mail through the Internet.

(i) As healthcare industry and other applicable security best practices evolve, Business Associate agrees to adjust its safeguards accordingly so that they continue to reflect the then-current industry best practices. To the extent that Business Associate has access to any part of CVS's data systems, Contractor shall comply with CVS's information security policies.

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

(k) Business Associate shall carry appropriate insurance to address the risks from its Processing of the Personal Information. CVS shall be named a certificate holder of such policies.

4. Permitted Uses and Disclosures of Protected Health Information.

(a) Subject to the limitations set forth in this Agreement, Business Associate may use and disclose Personal Information as necessary to provide its services as described in the Services Agreement.

(b) Business Associate may not de-identify Personal Information except as necessary to provide its services as described in the Services Agreement. Business Associate is prohibited from using or disclosing such de-identified information for its own purpose without the explicit written permission of CVS.

5. Term and Termination.

(a) The term of this Agreement shall continue for so long as the Services Agreement remains in effect, except that (i) Section 5(c) shall survive after the termination of the Services Agreement for as long as Business Associate retains any Protected Health Information; and (ii) any provision that by its nature survives termination shall so survive including, by way of example and not by way of limitation, Sections 2(c), 2(g), 2(l), 3(a) and (b), 5(c), 6 and 7(e) and (f).

(b) Upon CVS' determination that Business Associate has violated or breached a material term of this Agreement, CVS shall either: (1) provide an opportunity for Business Associate to cure the breach or end the violation, and terminate this Agreement and the Services Agreement if Business Associate does not cure the breach or end the violation within the time specified by CVS; or (2) immediately terminate this Agreement and the Services Agreement if it determines that Business Associate has breached a material term of this Agreement and cure is not possible.

(c) Effect of Termination. (1) Except as provided in paragraph (2) of this subsection *infra*, upon termination of the Services Agreement for any reason, Business Associate shall, at the election of CVS, return to CVS or destroy all Personal Information in its possession or that of its Subcontractors or agents. Business Associate and its agents and Subcontractors shall retain no copies of the Personal Information. (2) In the event that returning or destroying the Personal Information is infeasible, Business Associate shall provide to CVS written notification within ten (10) business days after termination of the Services Agreement of the conditions that make return or destruction infeasible. Upon agreement by CVS that return or destruction of the Personal Information is infeasible; Business Associate shall extend the protections of this Agreement to such Personal Information, and limit further uses and disclosures of it to those purposes that make the return or destruction infeasible, for so long as Business Associate or its agents or Subcontractors hold such Personal Information.

6. Indemnification and Liability.

(a) Business Associate will indemnify and hold harmless CVS and any of its officers, directors, employees, or agents from and against any claim, cause of action, liability, damage, cost or expense, including reasonable attorneys' fees and court or proceeding costs, arising out of or in connection with any breach of the terms of this Agreement, any Incident involving Personal Information under the control of Business Associate or its agents or Subcontractors or any person or entity under Business
Associate's direction or control, or any failure to perform its obligations with respect to Personal Information by Business Associate, it officers, employees, agents or any person or entity under Business Associate's direction or control.

(b) In the event of an Incident involving Personal Information under the control of Business Associate or its agents or Subcontractors or any person or entity under Business Associate's direction or control, Business Associate agrees to perform any reasonable mitigation or remediation services requested by CVS, and Business Associate further agrees to be responsible for costs and expenses including but not limited to: (i) reasonable costs of providing required notice to individuals affected by the Incident; (ii) reasonable costs of providing required notice to government agencies, credit bureaus, and/or other required entities; (iii) costs of providing individuals affected by the Incident with credit watch and protection services designed to prevent fraud associated with identity theft crimes for a specific period not to exceed twelve (12) months, except to the extent applicable law specifies a longer period for such credit protection services, in which case such longer period shall then apply; (iv) identity theft insurance of not less than one million dollars per person; (v) cost of providing reasonable call center support for such affected individuals for a specific period not less than ninety (90) calendar days, except to the extent applicable law specifies a longer period of time for such call center support, in which case such longer period shall then apply; (vi) reasonable fees associated with computer forensics work required for investigation activities related or relevant to the Incident; (vi) non-appealable fines or penalties assessed by governments or regulators; (viii) reasonable costs or fees associated with any obligations imposed by Applicable Law, including the HIPAA Rules, in addition to the costs and fees defined herein; and (ix) any other costs and expenses to undertake any other action both parties agree to be an appropriate response to the circumstances arising out of or in connection with any Incident.

7. Miscellaneous

(a) Business Associate agrees to take such action as CVS deems necessary to amend this Agreement from time to time to comply with the requirements of Applicable Law. If Business Associate disagrees with any such amendment proposed by CVS, it shall so notify CVS in writing no later than fifteen (15) business days after receipt of CVS' notice of the amendment. If the parties are unable to agree on an amendment, CVS may, at its option, terminate the Services Agreement.

(b) A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended, and as of its effective date.

(c) Any ambiguity in this Agreement shall be resolved to permit compliance with the HIPAA Rules.

(d) The terms and conditions of this Agreement shall override and control any conflicting term or condition of the Services Agreement and any other agreement between the parties. All non-conflicting terms and conditions of the Services Agreement and such other agreements remain in full force and effect.

(e) The parties agree that the remedies at law for a violation of the terms of this Agreement may be inadequate and that monetary damages resulting from such violation may not be readily measured. Accordingly, in the event of a violation by either party of the terms of this Agreement, the other party shall be entitled to immediate injunctive relief. Nothing herein shall prohibit either party from pursuing any other remedies that may be available to either of them for such violation.

(f) Business Associate represents that neither it nor its agents or Subcontractors will transfer, access or otherwise handle Personal Information outside the United States without the explicit prior written permission of CVS. Irrespective of where it performs its services or is domiciled, or any other factors affecting jurisdiction, Business Associate agrees, and shall require that its agents and contractors agree, to be subject to the laws of the United States, including the jurisdiction of the Secretary and the courts of the United States. Business Associate further agrees that all actions or proceedings arising in connection with this Agreement shall be tried and litigated exclusively in the United States in a venue in the State whose law governs the Services Agreement, and Business Associate waives any available jurisdictional defenses as they pertain to the parties' obligations under this Agreement or Applicable Law.

(g) During normal business hours, and with reasonable prior notice, CVS or its authorized representatives may audit, monitor and inspect Business Associate's and its agents or Subcontractors' facilities and equipment and any documents, information or materials in Business Associate's or its agents or Subcontractors' possession, custody or control; interview Business Associate's employees, agents, consultants and Subcontractors; and inspect any logs or documentation maintained by Business Associate to the extent relating in any way to Business Associate's obligations under this Agreement. An inspection performed pursuant to this Agreement shall not unreasonably interfere with the normal conduct of Business Associate's business. No such inspection by CVS as set forth herein shall relieve Business Associate of any of its obligations under this Agreement. Business Associate 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). Business Associate shall reasonably cooperate with any review for the VAP. In the event that the review under the VAP reveals material gaps or weaknesses in Business Associate's security program or its ability to Secure Personal Information, CVS shall be entitled to suspend transmission of Personal Information to Business Associate and suspend Business Associate's Processing of Personal Information until such issues are resolved to the satisfaction of CVS' Chief Privacy Officer and Chief Information Security Officer.

(h) Business Associate shall reasonably cooperate with CVS and with CVS' affiliates and representatives in responding to inquiries, claims and complaints regarding the Processing of the Personal Information.

(i) Business Associate shall carry appropriate insurance to address the risks from its Processing of the Personal Information. CVS shall be named a certificate holder of such policies.

(j) All Personal Information shall, as between the parties to this Agreement, at all times be and remain the sole property of CVS, and Business Associate shall not have or obtain any rights therein except to use and disclose such information for the purposes stated herein.

(k) Relationship of Parties. It is expressly agreed that Business Associate, its divisions, and its affiliates, including its employees and Subcontractors, are performing the services under this and the Services Agreement as independent contractors for CVS. Neither Business Associate nor of its affiliates, officers, directors, employees or Subcontractors is an employee or agent of CVS. Nothing in this Agreement shall be construed to create (i) a partnership, joint venture or other joint business relationship between the parties or any of their affiliates, or (ii) an agency relationship for purposes of Applicable Law.

****Signature to be administered between contractor and contractor employee. Informational only.****

Addendum B

Beacon Hill Staffing Group Personnel Covenants

Reference is made to that certain Vendor Agreement between Entellects Corp DBA Beedata Technologies Inc ("Contractor") and Beacon Hill Staffing Group, LLC ("Beacon Hill") dated on or about January 27, 2025 (the "Exhibit A Purchase Order"). Pursuant to the Exhibit A, Contractor agreed to provide certain services to Beacon Hill's "Client" who has engaged Beacon Hill for staffing services. Beacon Hill and its Client, CVS Pharmacy, Inc., have entered into certain Professional Services Agreement dated as of August 1, 2018 (the "CVS Agreement"). Pursuant to the CVS Agreement, CVS has required that Beacon Hill's contractor and its employees agree to certain flowdown provisions contained in the CVS Agreement, as set forth below. Therefore, in consideration of its continued employment by Contractor and Contractor's continued engagement by Beacon Hill and other valuable consideration, the undersigned Contractor employee agrees as follows:

1. Contractor employee agrees to be bound by the privacy and security requirements in Section 6.2 of the CVS Agreement, specifically the Data Privacy Addendum and the Security Addendum attached hereto.

2. Contractor employee agrees to be bound by the firewall requirements in Section 6.5 of the CVS Agreement, a copy of which are attached hereto.

3. Contractor employee agrees to be bound by the "Prohibited Services" provision of Exhibit A of the CVS Agreement, a copy of which is attached hereto.

Signature: [Contractor Signature]

Contractor Name: [Contractor Signer Name]

Date: [Contractor Signature Date]

CVS FLOW DOWN PROVISIONS

6.2 Privacy and Security Requirements

Vendor agrees and acknowledges that it is bound by the requirements defined in the Data Privacy and Security Addendum exhibits (the "Privacy Exhibits") that are attached to the Agreement as Exhibit C and Exhibit D and are incorporated herein by reference.

6.5 Firewall

Vendor acknowledges that CVS must maintain a firewall between the CVS retail pharmacy business (the "Retail Business") and the Caremark pharmacy benefits management business (the "PBM Business") to separate certain competitively sensitive information that each business possesses. Vendor agrees that, (1) Vendor will not knowingly transfer competitively sensitive information of the Retail Business to the PBM Business or allow the PBM Business to access such information, and (2) Vendor will not knowingly transfer competitively sensitive information of the PBM Business to the Retail Business or allow the Retail Business to access such Information.

SCOPE OF SERVICES

Vendor is authorized to provide any of the following Services to CVS. Actual Services to be provided will be detailed in a SOW agreed to and signed by the parties.

Authorized Services Provided: Enterprise Staff Augmentation Services.

Authorized CVS Business Areas/Departments: Enterprise.

Authorized CVS Information:
Confidential Information: Protected Health Information; Personal Information.

Prohibited Services
Notwithstanding anything to the contrary in herein, in the Agreement, or any bid package or SOW under the Agreement, Services that may involve Vendor's access to or materials containing Medicare Part D Information as defined in the Agreement, Nondisclosure Agreement, Business Associates Agreement, or Data Privacy and Security Requirements Exhibit, are not authorized under the Agreement. In the event Vendor receives access to said prohibited classes of information, even if such receipt is in error, Vendor shall immediately notify CVS upon discovery, shall be responsible for the security, confidentiality and protection of such information while in Vendor's possession, and shall return all relevant materials immediately as instructed by CVS.

THE AUTHORIZED SERVICES LISTED ABOVE ARE THE ONLY SERVICES AUTHORIZED BY THIS AGREEMENT. ANY ADDITIONAL SERVICES NOT LISTED AS AUTHORIZED SERVICES ABOVE, QUALIFYING AS PROHIBITED SERVICES OR OTHERWISE INVOLVING THE TYPES OF MEDICARE PART D INFORMATION AS DEFINED IN THE PRECEDING PARAGRAPH MUST BE AGREED TO BY BOTH PARTIES IN WRITING THROUGH AN AMENDMENT OF THIS AGREEMENT OR BY ENTERING INTO A SEPARATE AGREEMENT.

DATA PRIVACY ADDENDUM

This Data Privacy Addendum ("Data Addendum"), is hereby incorporated by reference into the Professional Services Agreement by and between CVS Pharmacy, Inc., a Rhode Island corporation, on behalf of itself and on behalf of its subsidiaries and Affiliates including without limitation Caremark Rx, L.L.C., (hereinafter called "CVS") and Vendor Name (herein the "Vendor"), with an effective date of August 1, 2018 (the "Agreement"). This Data Addendum is effective as the effective date of the Agreement ("the Effective Date"). Capitalized terms used in this Data Addendum have the meaning assigned in the Agreement unless otherwise defined herein. The terms of this Data Addendum supersede any conflicting terms of the Agreement.

Vendor agrees that it shall comply with the following provisions with respect to all Personal Information collected, used, transmitted or maintained for CVS and its affiliates. This Data Addendum stipulates privacy and confidentiality requirements.

3. Definitions.

1.1 "Applicable Law" shall mean any all national, state, regional and/or local laws, rules, regulations, security requirements and regulatory guidance applicable to either party's performance under the Agreement including but not limited to those applicable to the Processing of Personal Information.

1.2 "Incident" shall mean the use, disclosure or Processing of Personal Information in any form that is not authorized by this Data Addendum, or the interference with information systems containing Personal Information.

1.3 "Personal Information" has the meaning given by Applicable Law and includes any and all information or data (regardless of format and whether alone or in combination) that relates to an identified or identifiable individual; and is supplied to or Processed by or on behalf of Vendor in connection with the provision of the Services or otherwise for or on behalf of CVS Personal Information.

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

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

1.6 "Services" means any and all services that Vendor is required to perform under the Agreement that involves Processing of Personal Information.

4. Privacy Obligations.

2.1 Vendor shall Process Personal Information only as authorized and as necessary to perform the Services.

2.2 Vendor may disclose Personal Information to its employees and contractors, but only to the extent such individuals have a current purpose and need to access to and use of the Personal Information to perform the Services.

2.3 Vendor shall not disclose, transmit, or otherwise make Personal Information available to other third parties (including subcontractors) unless such Processing is explicitly required to perform the Services or has been explicitly authorized by CVS in writing.

2.4 Vendor agrees to ensure that any agent or subcontractor that may have access to Personal Information has agreed in writing to the same restrictions, conditions and requirements that apply through this Data Addendum to Vendor with respect to such information prior to obtaining such access. Vendor shall be liable to CVS for any acts, failures or omissions of such agents or subcontractor in violation of the requirements of this Data Addendum as if they were Vendor's own acts, failures or omissions, to the extent permitted by law, and any rights that CVS may exercise in connection with this Data Addendum in relation to Vendor, Vendor will ensure CVS may also exercise in relation to any such agent or subcontractor.

2.5 Vendor shall inform CVS in writing within five (5) business days of receipt of any request for access to any Personal Information or complaint received (i) from or on behalf of an individual who is the subject of the data; (ii) from any government official or agency (including any law enforcement agency) or (iii) from any other third party, other than requests that are required to be responded to as

part of the Services as described 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.

2.6 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 Data Addendum are contrary to those of the BAA such that it is impossible to comply with both, the more stringent, protective or restrictive provision shall apply.

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 agrees to report any Incident to CVS immediately, but in no event later than within two (2) business days, after it is discovered. An Incident shall be treated as discovered when any employee, director, officer, or agent of Vendor knows or should have known of such Incident by exercising reasonable diligence. The report shall be made by email to privacy.officer@cvshealth.com and shall contain the following information concerning the Incident: (i) a brief description of what happened, including the date of the Incident and the date of the discovery of the Incident, if known; (ii) the individuals affected; (iii) a description of the data elements involved in the Incident; (iv) any steps individuals should take to protect themselves from potential harm resulting from the Incident; (iv) a brief description of what Vendor is doing to investigate the Incident, to mitigate harm to individuals, and to protect against any further incidents; and (v) any other information reasonably requested by CVS. If such information is not available to Vendor at the time the Incident is required to be reported to CVS, Vendor shall continue to diligently investigate the Incident an provide such information to CVS promptly as it becomes available. The Vendor shall maintain complete records regarding the Incident for a minimum period of six (6) years or such longer period required by applicable law, and shall make such records available to CVS promptly upon request, but in no event later than within forty-eight (48) hours of such request.

3. Remediation and Mitigation

3.1 In the event of an Incident involving Personal Information under the control of Vendor or its agents or subcontractors or any person or entity under Vendor's direction or control, Vendor agrees to perform any reasonable mitigation or remediation services requested by CVS. Vendor further agrees to be responsible for all costs and expenses resulting from or related to the Incident, including but not limited to reasonable costs of providing required notices to individuals affected by the Incident, government agencies, credit bureaus, and/or other required entities.

4. Miscellaneous.

4.1 Vendor agrees to take such action as CVS deems necessary to amend this Data Addendum from time to time to comply with the requirements of applicable law. If Vendor disagrees with any such amendment proposed by CVS, it shall so notify CVS in writing no later than fifteen (15) business days after receipt of CVS's notice of the amendment. If the parties are unable to agree on an amendment, CVS may, at its option, terminate the Services Agreement.

4.2 Vendor's Processing shall comply with all applicable privacy laws and regulations, including (without limitation) Massachusetts 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth and similar state statutes.

4.3 Vendor shall, the extent applicable and consistent with the terms of this Data Addendum, abide by Vendor's own privacy notices and privacy policies and procedures.

4.4 Vendor represents that neither it nor its agents or subcontractors will transfer, access or otherwise handle Personal Information outside the United States without the explicit prior written permission of CVS.

4.5 The parties agree that the remedies at law for a violation of the terms of this Data Addendum may be inadequate and that monetary damages resulting from such violation may not be readily measured. Accordingly, in the event of a violation by either party of the terms of this Data Addendum, the other party shall be entitled to immediate injunctive relief. Nothing herein shall prohibit either party from pursuing any other remedies that may be available to either of them for such violation.

4.6 Any Personal Information provided to Vendor, or created, obtained, procured, used or accessed by Vendor in CVS's name or on CVS's

behalf, shall, as between the parties to this Agreement, at all times be and remain the sole property of CVS, and Vendor shall not have or obtain any rights therein except the right to use such data for the purposes stated herein.

CVS PHARMACY, INC.
SECURITY ADDENDUM

A. Vendor agrees to:

(1) Employ essential current industry practice security controls and tools to monitor its information processing systems and log key events such as user activities (including root or administrative access), exceptions, successful and unsuccessful logins, access to audit logs, unauthorized information processing activities, suspicious activities and information security events;

(2) Ensure that neither it nor any of its employees or contractors ("Workforce") will place Protected Health Information or Personal Information on portable computing/storage devices which are not owned by Vendor;

(c) "Protected Health Information" or "PHI" shall have the same meaning as such term is defined in 45 CFR 160.103, but limited to information created, accessed or received for or on behalf of CVS, or in the course of providing services for CVS;

(d) "Personal Information" has the meaning given by Applicable Law and includes any and all information or data (regardless of format and whether alone or in combination) that relates to an identified or identifiable individual; and is supplied to or Processed by or on behalf of Vendor in connection with the provision of the Services or otherwise for or on behalf of CVS;

(3) Ensure that data files containing PHI and/or PII are not saved on public or private computers while accessing corporate e-mail through the Internet;

(4) Secure all electronic PHI and/or PII in motion;

(5) Secure any PHI and/or PII at rest that is placed or stored on portable devices 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);

(6) Secure all electronic PHI and PII at rest, including ensuring that all electronic PHI held at rest shall be rendered unreadable by unauthorized parties using strong encryption technologies;

(7) Dispose of all PHI and/or PII in a Secure manner, including the permanent removal of all PHI and/or PII from such media or devices before making such electronic media or devices available for re-use;

(8) Make log events available for monitoring to CVS or a managed security service provider as designated by CVS;

(9) Regularly back up activity logs to a secure central location, protected against tampering and unauthorized access;

(10) Retain activity logs in accordance with regulatory requirements;

(11) Perform regular, routine log reviews and take necessary actions to protect against unauthorized access or misuse;

(12) Comply with all applicable regulatory requirements related to monitoring and logging activities;

(13) Ensure that the clocks of all relevant information processing systems will be synchronized using an authoritative national or international time source;

(14) Incorporate date and time stamp into log entries;

(15) Employ, monitor, and keep up to date intrusion detection systems and intrusion prevention systems to monitor all network traffic and alert personnel to suspected security events;

(21) Ensure access to Vendor applications accessible over un-trusted or open networks are controlled and restricted by a defined security perimeter;

(22) Appropriate security barriers including entry controls, authentication controls, malicious or hostile software detection are applied. Access to applications is restricted to authorized parties using authorized protocols.

(23) Obtain certification that its information security safeguards meet or exceed a defined industry information security standard and maintain its safeguards in compliance with such certification requirements and obligations;

(24) Provide to CVS, at CVS's request, a list of its Workforce who have (or have had) access to the Protected Health Information and the work location of each such individuals; and

(25) Submit to controls testing by CVS, or at the sole cost of the Vendor a mutually agreed upon third party, and provide evidence at least annually, demonstrating a process for threat & vulnerability management, including:

(e) Regularly scheduled internal and external system, application, and network vulnerability scans;

(f) Results of network and application layer penetration tests

(g) Results of secure application source code scanning and analysis review; and

(h) Vendor agrees to remediate vulnerabilities to the reasonable satisfaction of CVS.

D. Vendor represents that neither it nor its agents or Subcontractors will transfer, access or otherwise handle PHI and/or PII outside the United States without the explicit prior written permission of CVS.

E. Before obtaining access to or receiving any PHI and/or PII from CVS, Vendor shall 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).

(e) Any Vendor representations made during the VAP or Vendor responses provided to questions as part of the VAP are hereby incorporated into the Master Services Agreement and Vendor shall be obligated to comply with and honor such representations as if they were part of the Agreement.

(f) Vendor shall reasonably co-operate with any review for the VAP.

(g) If the review under the VAP identifies material gaps or weaknesses in Vendor's security program or its ability to Secure PHI and/or PII, CVS shall be entitled to suspend Vendor's access to or use of CVS PHI and/or PII until such issues are resolved to the satisfaction of CVS's Chief Privacy Officer and Chief Information Security Officer.

(h) During the term of this Addendum, CVS may periodically, but no more frequently than once every two years, request that Vendor complete a new VAP. If any subsequent annual review under the CVS VAP identifies any material gaps or weaknesses in Vendor's security program or its ability to Secure PHI and/or PII, CVS shall be entitled to suspend Vendor's access to or use of CVS PHI and/or PII until such issues are resolved to the satisfaction of CVS's Chief Privacy Officer and Chief Information Security Officer.

Addendum C

CVS Travel Policy

1.0 Air Travel

1.1 Fares and Service Levels

(i) Non-refundable tickets must be booked when available.

(ii) When a flight is within one (1) hour of the preferred arrival time and within one (1) hour of a direct flight's landing time or both, Vendor must accept the lowest priced logical flight including connections, direct, and non-stop flights.

(iii) Coach class will be used for domestic flights.

(iv) First Class travel is not permitted unless approved by CVS in advance.

(v) International flights may be booked in business class and must be booked fourteen (14) days in advance to allow for a security check by Loss Prevention.

(vi) CVS will not reimburse for chartered flights.

2.0 Tickets

(i) Airline tickets are non-transferable.

(ii) E-tickets should be issued for travel. Additional fees for paper-based tickets are not reimbursable.

3.0 Frequent Flyer Programs and Air Clubs

(i) Vendor should not allow the potential for earning additional frequent flyer mileage influence their airline choice.

(ii) Airline Club memberships will not be reimbursed.

4.0 Auto Rentals

4.1. Preferred Auto Rental Vendor

(i) National and Enterprise are the current CVS preferred auto rental vendors

(ii) Negotiated rental agreements should be used whenever possible and are assessable via the following site: http://www.enterprise.com/car_rental/deeplinkmap.do?bid=028&refId=CVS

(iii) Insurance coverage is not included in the rates provided by National or Enterprise

(iv) Rental of compact or mid-sized cars is required. Full size vehicles are allowed for groups traveling together.

4.2. Fuel Expenses for Auto Rental

To avoid the higher cost of gasoline charged by auto rental providers, Vendor must return the rental car with a full gas tank unless doing so would result in missing flights.

4.3. Traffic Fines & Violations

Traffic fines, parking violations, theft, and loss or damage of personal items and effects are not reimbursable.

5.0 Lodging

5.1 Hotel

(i) Vendor is expected to exercise good judgment in selecting suitable accommodations

(ii) Hotel rates of $300 or more per night must be approved by CVS in advance

(iii) CVS preferred hotel chain is Marriott. To take advantage of our negotiated rates, please call the hotel and request "CVS" rates.

(iv) Vendor should make every effort to book one of CVS' preferred hotels.

5.2 Express Check-out

If Vendor chooses to use express check-out offered by hotels, Vendor must submit proof of payment for any express check-out receipts showing an open balance.

6.0 Meals

6.1 Personal Meals

(i) CVS will reimburse Vendor for meals when travel requires an overnight stay or eight (8) hours or more of travel away from home base area.

(ii) Vendor should always use good judgment and avoid extravagance.

(iii) Personal meals should be reasonably priced and itemized on your expense report accompanied by an original receipt with the restaurant's name clearly printed. CVS will not reimburse more than seventy-five dollars ($75 per) day for personal meals.

(iv) Tips will not be reimbursed more than twenty percent (20%).

(v) Vendor must submit detailed receipts with the name of the restaurant clearly imprinted on the receipt along with the credit card slip as proof of payment. A detailed receipt should be requested from the restaurant at time of payment. Submission of only a credit card slip will not be accepted.

(vi) Personal meals under twenty-five dollars ($25) do not need a detailed receipt.

Addendum D

Background and Drug Testing Standards

BACKGROUND CHECK AND DRUG TESTING REQUIREMENTS AND STANDARDS
All Associates meeting the requirements of Section 1 of this Exhibit must comply with the following criteria:

(i) A "9-Panel Drug Test" consisting of a specimen test for known amphetamines, marijuana, cocaine, opiates, barbiturates and other potentially illegal drugs no more than three (3) days before the effective date of an assignment.

(ii) Validation of educational experience inclusive of the name of the institution and the degree or certification, proof of license, letters of reference or other such written testimony as deemed pertinent by CVS, in its sole discretion, to the work for hire.

(iii) Validation of each Associate's employment history.

(iv) Validation of the social security number for each Associate with access to CVS facilities or CVS Sensitive Information.

(v) Confirmation that each Associate with access to CVS facilities or CVS Sensitive Information (i) is not an Ineligible Person as such term is defined in the Agreement, (ii) has not been charged with a criminal offense that falls within the ambit of 42 U.S.C. Section 1320a-7(a) or Section 1320a-7(b)(l)- (3) and (iii) has not been proposed for exclusion, debarment, suspension, or other eligibility from any Federal health care program or Federal procurement or non-procurement program. This requirement shall include but not be limited to checks with: the Office of Inspector General, System for Award Management (SAM), and the Office of Foreign Assets Terror Watch List.

(vi) The background check shall include but not be limited to: (1) a seven-year address history, (2) a seven year county of residence criminal conviction search, (3) a national federal criminal database check , and (4) in each of (2) and (3) above, containing no felony or misdemeanor conviction that related to fraud or theft (including but not limited to, shoplifting, larceny, embezzlement, forgery, credit card fraud, or check fraud), the disposition of which is within seven years, as allowed by law.

(vii) A Motor Vehicle Report and an active Driver's License shall be required for all Associates operating a motor vehicle at any CVS location.

Addendum E

Insurance Requirements

Insurance
During the Term of this Agreement, Vendor shall, at its expense, carry and maintain:

1. Workers Compensation and Employers Liability Insurance meeting minimum statutory requirements,

2. Commercial Umbrella and/or Employers Liability Limits of no less than $1,000,000 each accident for bodily injury and $1,000,000 each employee for bodily injury by disease,

3. Commercial General Liability (CGL) and/or Umbrella Liability insurance written on ISO Occurrence form CG 00 01 12 07 or equivalent, written on an occurrence form, with a limit of not less than $2,000,000 each occurrence, $4,000,000 General Aggregate and $4,000,000 Products Completed Operations Aggregate

4. Automobile Liability and/or Umbrella Liability insurance with limits of not less than $1,000,000 each accident.

Professional Liability Insurance
In addition to the insurance required above, and prior to its performance under this Agreement, Vendor shall, at its own expense, procure Professional Liability/Errors and Omissions Insurance, or such other insurance as is necessary to ensure coverage for any and all acts, omissions, and errors of Vendor with respect to all Services performed and provided under this Agreement. This insurance should provide limits of not less than $2,000,000 per claim. Such insurance should also include coverage for the wrongful disclosure of any third party's proprietary information including, without limitation, trade secrets.

Intellectual property infringement coverage with a limit of not less than USD$2,000,000/claim. Such insurance shall include, without limitation, coverage for infringement upon any third party's proprietary information, copyright and trademark;

Privacy liability coverage with a limit of not less than USD$5,000,000/claim. Such insurance shall include, without limitation, coverage for unauthorized access, denial of service attacks, breach of privacy and the failure to protect and disclosure of personally identifiable information, payment card information and health information; violation of any federal, state or local law or regulation in connection with the protection of information including fines and penalties to the extent allowed by applicable law; notification and crisis management costs, identity theft monitoring and regulatory defense; disclosure of any third party's proprietary information including, without limitation, trade secrets, and; liability for interruption of client or any third party's business including, without limitation, claims for loss of use and loss of profits;
Media liability coverage, including coverage for online and offline media to the extent not afforded under the Commercial General Liability Insurance required above, with a limit of not less than USD$5,000,000/claim. Such insurance shall include, without limitation, coverage for invasion of privacy and advertising injury including, without limitation, libel, slander, and defamation;

Commercial Crime insurance in the amount of $5,000,000/occurrence, including coverage for computer fraud, funds transfer fraud and employee dishonesty; and

Insurance required under this section (if provided on a claims made form) shall have a retroactive date no later than the Effective Date of this Agreement. Vendor shall maintain in effect such insurance during the entire Term of this Agreement, and upon expiration or termination of this Agreement, Vendor shall maintain in effect such insurance for a period of not less than thirty-six (36) months.