BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is entered into and is in effect as of __-_____(mm/dd/yyyy), by and between **HARVARD PILGRIM HEALTH CARE, INC.**, a Massachusetts non-profit corporation licensed as a health maintenance organization under the laws of Massachusetts, on behalf of itself and all present and future affiliates (hereinafter referred to as the "Covered Entity") and

_____

[Broker], on behalf of itself as an individual broker or broker organization, and if a broker organization, also on behalf of any present and future employees (hereinafter referred to as "Business Associate") (collectively the "Parties").

WHEREAS, the Parties wish to enter into or have entered into an arrangement ("Arrangement") whereby Business Associate will provide certain services to Covered Entity and, in providing those services, Business Associate may create, receive, maintain or transmit from, or on behalf of, Covered Entity Protected Health Information ("PHI") (defined below) and may create, receive, maintain or transmit Electronic Protected Health Information ("EPHI")(defined below)(PHI and EPHI are collectively referred to herein as PHI or Protected Health Information; EPHI will be used when only EPHI is being referenced);

WHEREAS, Covered Entity and Business Associate intend to protect the privacy and provide for the security of any PHI which shall be disclosed to or created by Business Associate pursuant to the Arrangement, in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the implementing regulations at 45 CFR Parts 160, 162, and 164 promulgated by the United States Department of Health and Human Services ("HIPAA Regulations"), the requirements of the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (the "HITECH Act") that are applicable to business associates, along with any guidance or regulations issued by the U. S. Department of Health and Human Services ("DHHS"), and other applicable laws;

WHEREAS, as part of the HIPAA Regulations, the Privacy and Security Rule (defined below) requires Business Associate to enter into a contract containing specific provisions intended to preserve the confidentiality and security of PHI obtained by Business Associate in the course of its business relationship with Covered Entity (defined below) prior to any disclosure of the PHI to Business Associate. The specific provisions are set forth in, but not limited to, Title 45, Sections 164.306, 164.308(b), 164.314(a) and (b), 164.502(e) and 164.504(e) of the Code of Federal Regulations and are applicable to this Agreement; and

WHEREAS, Business Associate agrees to comply with all other applicable federal and state laws for the protection of personal information and the reporting of security breach

incidents, including the General Laws of Massachusetts Chapter 93H, and implementing regulations at 201 CMR 17.00, New Hampshire Revised Statutes Chapter 359-C, Maine Revised Statutes Chapter 210-B, and Connecticut General Statutes, Chapters 669 (section 36A-701B) and 743dd (hereinafter "the applicable state laws").

NOW THEREFORE, in consideration of the mutual promises below, and the exchange of PHI pursuant to the terms of this Agreement, the Parties agree as follows:

1.0 **DEFINITIONS**

As used in this Agreement, the following terms shall have the indicated meaning. Capitalized terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the HIPAA Regulations and the HITECH Standards (defined below), or for Personal Information, the definition found in the applicable state laws. The definitions below which set forth a reference to the Code of Federal Regulations are defined HIPAA terms, and such definitions are incorporated herein as though set forth in full. A change to the HIPAA Regulations or the HITECH Standards which modifies any defined term, or which alters the regulatory citation for the definition shall be deemed incorporated into this Agreement.

1.1 **Arrangement** means the agreement, either with or without a written contract, between Covered Entity and Business Associate, whereby Business Associate provides or will provide certain services to Covered Entity and, in providing those services, may have access to PHI.

1.2 **Authorization** shall have the meaning given to the term under the Privacy and Security Rule, including, but not limited to, 45 CFR Section 164.508.

1.3 **Breach** shall have the same meaning as the term "breach" in Section 13400 of the HITECH Act and shall include the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of such information. For purposes of Personal Information, the term "Breach of Security" shall have the meaning given in the applicable state laws.

1.4 **Business Associate** shall mean _____[Broker]. Where the term "business associate" appears without initial capital letters, it shall have the meaning given to such term under the Privacy and Security Rule, including, but not limited to, 45 CFR Section 160.103.

1.5 **Covered Entity** shall mean Harvard Pilgrim Health Care, Inc., as defined. It shall also have the meaning given to the term under the Privacy and Security Rule, including, but not limited to, 45 CFR Section 160.103.

1.6 **Data Aggregation** shall have the meaning given to the term under the Privacy and Security Rule, including, but not limited to, 45 CFR Section 164.501.

1.7 **Designated Record Set** shall have the meaning given to the term under the Privacy and Security Rule, including, but not limited to, 45 CFR Section 164.501.

1.8 **Electronic Protected Health Information ("EPHI")** shall have the meaning given to the term Electronic Protected Health Care Information under the Privacy and Security Rule, including, but not limited to, 45 CFR Section 160.103.

1.9 **Encryption** means the transformation of data through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, unless a higher standard is defined by the appropriate regulatory body under the applicable state laws.

1.10 **Health Care Operations** shall have the meaning given to the term under the Privacy and Security Rule, including, but not limited to, 45 CFR Section 164.501.

1.11 **HITECH Standards** means the privacy, security and security Breach notification provisions applicable to a Business Associate under the HITECH Act.

1.12 **Individual** shall have the meaning given to the term under the Privacy and Security Rule, including, but not limited to, 45 CFR Section 164.501. It shall also include a person who qualifies as a personal representative in accordance with 45 CFR Section 164.502(g).

1.13 **Personal Information** will have the meaning given by applicable state laws in states in which Business Associate receives Personal Information.

1.14 **Privacy and Security Rule** shall mean the Standards for Privacy of Individually Identifiable Health Information and the Security Standards for the Protection of Electronic Protected Health Information that is codified at 45 CFR parts 160 and 164.

1.15 **Protected Health Information ("PHI")** means any information, whether oral or recorded in any form, or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe that

the information can be used to identify the individual, and shall have the meaning given to the term under the Privacy and Security Rule, including, but not limited to, 45 CFR Section 164.501.

1.16 **Required by Law** shall have the meaning given to the term under the Privacy and Security Rule, including but not limited to, 45 CFR Section 164.501.

1.17 **Security Incident** shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of EPHI, or interference with system operations in an information system.

1.18 **Security Standards** shall mean those security standards promulgated or to be promulgated pursuant to HIPAA and other applicable federal or state regulations or statutes.

1.19 **Unsecured Protected Health Information** or Unsecured PHI shall mean PHI that is not secured through the use of a technology or methodology specified by the Secretary in guidance or as otherwise defined in Section 13402(h) of the HITECH Act.

2.0 Obligations of Business Associate

2.1 **Permitted Use and Disclosure of Protected Health Information.** Business Associate may use and disclose PHI only as required to satisfy its obligations under the Arrangement or this Agreement, as permitted herein, as allowed by HIPAA and HIPAA Regulations, or as Required by Law, but shall not otherwise use or disclose any PHI. Business Associate shall not, and shall ensure that its directors, officers, employees, contractors and agents do not, use or disclose PHI in any manner that would constitute a violation of the Privacy and Security Rule or the HITECH Act if done by the Covered Entity, except that Business Associate may use PHI if necessary (i) for the proper management and administration of Business Associate, (ii) to carry out the legal responsibilities of Business Associate, or (iii) to provide Data Aggregation services relating to the Health Care Operations of the Covered Entity. Business Associate further represents that, to the extent it requests Covered Entity to disclose PHI to Business Associate such request will only be for the minimum PHI necessary for the accomplishment of Business Associate's purpose.

2.2 **Safeguarding PHI and Personal Information.** Business Associate shall use any and all appropriate safeguards to prevent use or disclosure of PHI and/or Personal Information other than as permitted by this Agreement. Business Associate further agrees to use appropriate administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of any PHI and/or Personal Information that Business Associate

creates, receives, maintains, or transmits on behalf of Covered Entity, in accordance with the HIPAA Regulations, the HITECH Standards, and for Personal Information, the applicable state laws in states in which Business Associate receives Personal Information. More specifically, to comply with the HIPAA Security Standards for PHI, the requirements of the HITECH Act, and to applicable state laws protecting Personal Information, Business Associate agrees that it shall: (i) Develop and implement policies and procedures that meet the Security Standards documentation requirements of the HITECH Act; (ii) As also provided for in Section 2.5 below, ensure that any agent, including a subcontractor, to whom it provides such PHI or Personal Information agrees to implement reasonable and appropriate safeguards to protect it; (iii) Report to Covered Entity, any Security Incidents or Breaches of Security of which Business Associate becomes aware that result in the unauthorized access, use, disclosure, modification, or destruction of the Covered Entity's PHI or Personal Information, (hereinafter referred to as "Successful Security Incidents"). Business Associate shall report Successful Security Incidents to Covered Entity as specified in Section 2.4.3, and upon Covered Entity's request, shall provide access to and copies of documentation regarding Business Associate's safeguards for PHI; (iv) For any other Security Incidents that do not result in unauthorized access, use, disclosure, modification, or destruction of PHI (including, for purposes of example, and not for purposes of limitation, pings on Business Associate's firewall, port scans, attempts to log onto a system or enter a database with an invalid password or username, denial-of-service attacks that do not result in the system being taken off-line, or malware such as worms or viruses)(hereinafter "Unsuccessful Security Incidents"), Business Associate shall, upon Covered Entity's written request, report to the Covered Entity in accordance with the reporting requirements identified in Section 2.4.3; (v) Encrypt all PHI and/or Personal Information stored on laptops or other personal devices, encrypt all transmitted records and files containing PHI and/or Personal Information that will travel across public networks, and encrypt all PHI and/or Personal Information to be transmitted wirelessly; and (vi) Business Associate agrees that this Agreement constitutes its representation that it has a written, comprehensive information security program that meets its obligation to safeguard Personal Information in its possession as required by the applicable state laws.

2.3 **Mitigation of Harmful Effects.** Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI or Personal Information by Business Associate in violation of the requirements of this Agreement.

2.4 **Breach of Privacy or Security Obligations.**

2.4.1 **Notice and Reporting of Violations.** Business Associate shall notify and report to Covered Entity in the manner described herein any use or disclosure of PHI or Personal Information in violation of this Agreement by Business Associate or any of its officers, directors, employees, contractors or agents.

2.4.2 **Notice to Covered Entity.** Business Associate will notify Covered Entity following discovery and without unreasonable delay but in no event later than five (5) business days following discovery, any Breach of Unsecured Protected Health Information as these terms are defined by the HITECH Act and any implementing regulations, or any Breach of Security under the applicable state laws. Business Associate shall cooperate with Covered Entity in investigating the Breach and in meeting Covered Entity's obligations under the HITECH Act and any other security breach notification laws. Business Associate shall follow its notification to the Covered Entity with a report that meets the requirements outlined immediately below.

2.4.3 **Reporting to Covered Entity.** (i) For Successful Security Incidents and any other use or disclosure of PHI or Personal Information that is not permitted by this Agreement, the Arrangement, by applicable law, or without the prior written approval of the Covered Entity, Business Associate, without unreasonable delay, but in no event later than ten (10) business days after Business Associate learns of such Successful Security Incident or non-permitted use or disclosure, shall provide Covered Entity a report that will: (a.) Identify, if known, each individual whose Unsecured Protected Health Information or Personal Information has been, or is reasonably believed by Business Associate to have been accessed, acquired, or disclosed during such Breach; (b) Identify the nature of the non-permitted access, use, or disclosure, including the date of the incident and the date of discovery; (c) Identify the PHI or Personal Information accessed, used, or disclosed (e.g., name; social security number, date of birth); (d) Identify who made the non-permitted access, use, or received the non-permitted disclosure; (e) Identify what corrective action Business Associate took or will take to prevent further non-permitted access, use or disclosure; (f) Identify what Business Associate did or will do to mitigate any deleterious effect of the non-permitted access, use, or disclosure; and (g) Provide such other information, including a written report, as the Covered Entity may reasonably request. (ii) For Unsuccessful Security Incidents, Business Associate shall provide Covered Entity, upon its written request, a report that: (a) identifies the categories of Unsuccessful Security

Incidents as described in Section 2.2; (b) indicates whether Business Associate believes its current defensive security measures are adequate to address all Unsuccessful Security Incidents, given the scope and nature of such attempts; and (c) if the security measures are not adequate, the measures Business Associate will implement to address the security inadequacies.

2.4.4 **Reporting by Covered Entity.** Where a Breach relates to PHI, if Covered Entity determines pursuant to section 4.2 of this Agreement that termination of this Agreement is not feasible, in Covered Entity's sole discretion, then Covered Entity shall have the right to report Business Associate's Breach to the Secretary of the Department of Health and Human Services.

2.5 **Agreements by Third Parties.** Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides or transmits PHI and/or Personal Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

2.6 **Access to Information.** Within ten (10) days of a request by Covered Entity for access to PHI about an Individual contained in a Designated Record Set, Business Associate shall make available to Covered Entity such PHI in order to enable Covered Entity to meet the requirements of 45 CFR Section 164.524, and where applicable, the requirements of the HITECH Act and any related implementing regulations. In the event any Individual requests access to his or her PHI directly from Business Associate, it shall within two (2) days forward such request to Covered Entity so that Covered Entity can comply with the request. Business Associate shall not provide direct access to any Individual who requests access to his or her PHI. Any denials of access to the PHI requested shall be the responsibility of Covered Entity.

2.7 **Availability of Protected Health Information for Amendment.** Within thirty (30) days of receipt of a request from Covered Entity for the amendment of an Individual's PHI or a record regarding an individual contained in a Designated Record Set, Business Associate shall provide such information to Covered Entity for amendment and shall incorporate any such amendments in the PHI as required by 45 CFR Section 164.526. Any denials of requested amendments shall be the responsibility of Covered Entity.

2.8 **Accounting of Disclosures.** Within twenty (20) days of making a disclosure of PHI, other than disclosures excepted under 45 CFR Section 164.528(a), Business Associate shall report such disclosure to Covered Entity in writing as provided for in 45 CFR Section 164.528 or the HIPAA Regulations, and

where so required by the HITECH Act and/or any implementing regulations. At a minimum, Business Associate shall provide the following information for each disclosure: (i) the date of the disclosure; (ii) the name of the entity or person who received the PHI and, if known, the address of such entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of such disclosure which includes an explanation of the basis for such disclosure. In the event that an Individual's request for an accounting is delivered directly to Business Associate, it shall within five (5) days forward such request to the Covered Entity so that Covered Entity can comply with the request. Such information must be maintained by Business Associate and its agents and subcontractors for a period of six (6) years from the date of each disclosure.

2.9 **Auditing, Inspections and Enforcement.** Upon reasonable notice, Business Associate agrees to make its internal practices, books and records relating to the use or disclosure of PHI available to Covered Entity and the Secretary of the Department of Health and Human Services, or the Secretary's designee, for purposes of determining Covered Entity's compliance with the Privacy and Security Rule. Business Associate shall provide appropriate training regarding the requirements of this Agreement to any employee accessing, using or disclosing PHI and shall develop and implement a system of sanctions for any employee, agent or subcontractor who violates this Agreement.

2.10 **Indemnification.** Business Associate shall indemnify and hold harmless Covered Entity from and against any and all losses, expense, damage or injury that Covered Entity sustains as a result of, or arising out of a breach of this Agreement by Business Associate or its agents or subcontractors, including but not limited to any unauthorized use or disclosure of PHI.

2.11 **Notice of Request for Data.** Business Associate agrees to notify Covered Entity within five (5) days of Business Associate's receipt of any request, subpoena, or judicial or administrative order to disclose PHI. To the extent the Covered Entity decides to assume responsibility for challenging the validity of such request, subpoena or order, Business Associate agrees to cooperate with Covered Entity in such challenge.

2.12 **Compliance with HITECH Standards.** Business Associate understands that it must comply with the security provisions made applicable to Business Associates by HITECH section 13401 and the privacy provisions made applicable to Business Associates by HITECH section 13404; in addition, Business Associate shall comply with the HITECH Standards, including, but not limited to: (i) compliance with the requirements regarding minimum necessary under HITECH section 13405(b); (ii) requests for restrictions on use or disclosure to health plans for payment or health care operations purposes when the provider has been paid out of pocket in full consistent

with HITECH section 13405(a); (iii) the prohibition of sale of PHI without authorization unless an exception under HITECH section 13405(d) applies; (iv) the prohibition on receiving remuneration for certain communications that fall within the exceptions to the definition of marketing under 45 CFR section 164.501 unless permitted by this Agreement and section 13406 of HITECH; (v) the requirements relating to the provision of access to certain information in electronic access under HITECH section 13405(e); (vi) compliance with each of the Standards and Implementation specifications of 45 CFR sections 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), 164.312 (Technical Safeguards) and 164.316 (Policies and Procedures and Documentation Requirements); and (vii) the requirements regarding accounting of certain disclosures of PHI maintained in an Electronic Health Record under HITECH section 13405(c).

2.13 **Acknowledgement of Direct Liability.** Business Associate acknowledges that it is directly liable under the Final HIPAA Rule and subject to penalties in accordance with the HIPAA Rules for making uses and disclosures of Protected Health Information that are not authorized by its contract or required by law, and that it is directly liable and subject to civil penalties for failing to safeguard EPHI in accordance with the HIPAA Security Rule.

3.0 Covered Entity's Obligations.

3.1 **Notice of Privacy Practices.** Covered Entity shall provide Business Associate with the notice of any privacy practices that Covered Entity produces in accordance with 45 CFR Section 164.520, as well as any changes to such notice. Business Associate shall not distribute its own notice, if any, to Individuals, without the prior written consent of Covered Entity.

3.2 **Revocation of Authorization by Individual.** Covered Entity agrees to inform Business Associate of any change to, or revocation of, an Individual's Authorization to use or disclose PHI to the extent that such change may affect Business Associate's use or disclosure of PHI, within a reasonable period of time after Covered Entity becomes aware of such change.

3.3 **Restrictions on Use and Disclosure.** Covered Entity agrees to notify Business Associate of any restrictions to the use or disclosure of PHI agreed to by Covered Entity in accordance with 45 CFR Section 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

3.4 **Permissible Requests.** Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy and Security Rule if done by Covered Entity.

3.5 **Safeguards.** Covered Entity shall use appropriate safeguards in accordance with 45 CFR Section 164.306 to ensure the security of PHI provided to Business Associate pursuant to the Arrangement and this Agreement, until such PHI is received by Business Associate.

4.0 Termination of Agreement.

4.1 **Term.** This Agreement shall be effective from the Effective Date until all PHI provided by or received or created for Covered Entity is destroyed or returned to Covered Entity, or if it is infeasible to return or destroy PHI, protections are extended to such PHI in accordance with the terms of this Agreement. The term of this Agreement shall also end upon termination of the underlying Arrangement, subject, however, to the requirements of this section 4.0 for return or destruction of all PHI.

4.2 **Termination Upon Breach of Provisions Applicable to Protected Health Information or Personal Information.** Any other provision of this Agreement notwithstanding, this Agreement and the Arrangement may be terminated by Covered Entity upon ten (10) days prior written notice to Business Associate in the event that Business Associate materially breaches any obligation of this Agreement and fails to cure the breach within such ten (10) day period.

4.3 **Return or Destruction of Protected Health Information and Personal Information upon Termination.** Upon termination of this Agreement and the Arrangement, Business Associate shall either return to Covered Entity or destroy all PHI and Personal Information in Business Associate's possession or in the possession of its agents or subcontractors. Business Associate shall not retain any copies of PHI or Personal Information. Notwithstanding the foregoing, if Business Associate determines that returning or destroying PHI and/or Personal Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of PHI and/or Personal Information is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and/or Personal Information and limit further uses and disclosures of such PHI and/or Personal Information to those purposes that make return or destruction infeasible, for so long as Business Associate maintains such PHI and/or Personal Information. If Business Associate elects to destroy all PHI and/or Personal Information, it shall certify in writing to Covered Entity that such PHI and/or Personal Information has been destroyed.

4.4 **Remedies.** Notwithstanding any rights or remedies set forth in this

Agreement or provided by law, Covered Entity retains all rights to seek injunctive relief to prevent or stop the unauthorized use or disclosure of PHI and/or Personal Information by Business Associate, any of its agents or subcontractors, or any third party who has received PHI and/or Personal Information from Business Associate.

4.5 **Judicial or Administrative Proceedings.** Either Party may terminate this Agreement, effective immediately, if (i) the other Party is named as a defendant in a criminal proceeding for a violation of HIPAA, the HIPAA Regulations, the HITECH Act, or other security or privacy laws, or (ii) a finding or stipulation that the other party has violated any standard or requirement of HIPAA, the HIPAA Regulations, the HITECH Act or other security or privacy laws is made in any administrative or civil proceeding in which the Party has been joined.

5.0 Miscellaneous

5.1 **Relationship of the Parties.** None of the provisions of this Agreement are intended to create or shall be deemed to create any relationship between the Parties other than that of independent parties contracting with each other solely for the purposes of effecting the provisions of this Agreement and any other Arrangement between the Parties.

5.2 **Ownership of Protected Health Information and Personal Information.** As between Covered Entity and Business Associate, Covered Entity holds all right, title and interest in and to any and all PHI and/or Personal Information received by Business Associate from, or created or received by Business Associate on behalf of, Covered Entity, and Business Associate does not hold, and will not acquire by virtue of this Agreement or by virtue of providing any services or goods to Covered Entity in the course of fulfilling its obligations pursuant to the Arrangement, any right, title or interest in or to such PHI and/or Personal Information. Except as specified in section 2.1 of this Agreement, Business Associate shall have no right to compile or distribute any statistical analysis or report utilizing such PHI and/or Personal Information derived from such PHI and/or Personal Information, any aggregate information derived from such PHI and/or Personal Information, or any other health and medical information obtained from Covered Entity.

5.3 **No Third Party Beneficiaries.** Nothing expressed or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person or entity, other than Covered Entity, Business Associate and their respective successors and assigns, any rights, remedies, obligations or liabilities whatsoever.

5.4 **Amendment to Comply With Law.** Business Associate and Covered Entity agree to amend this Agreement to the extent necessary to allow either Party to comply with the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule and other applicable state and federal laws relating to the security or confidentiality of PHI and/or Personal Information. Business Associate and Covered Entity will fully comply with all applicable standards and requirements of such federal or state regulations or statutes. To the extent that any amendment of such laws requires changes to this Agreement, Covered Entity shall provide written notice to Business Associate of such changes and this Agreement shall be automatically amended to incorporate the changes set forth in the written notice provided by Covered Entity to Business Associate unless the Business Associate objects to such changes in writing within fifteen (15) days of receipt of such notice. If Business Associate objects in a timely manner to such amendment, the Parties shall work in good faith to reach agreement on a change to the Agreement that complies with the amendment of such laws. If the Parties are unable to reach agreement on a change to the Agreement within thirty (30) days of the date that Covered Entity receives written objection from Business Associate, then either Party may terminate this Agreement upon written notice of such termination.

5.5 **Other Amendments.** Any other amendment to this Agreement unrelated to compliance with applicable law and regulations shall be effective only upon execution of a written agreement between the Parties.

5.6 **Waiver.** No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation on any other occasion.

5.7 **Survival.** The respective rights and obligations of Business Associate under Section 4.3 of this Agreement shall survive the termination of this Agreement and the underlying Arrangement.

5.8 **Notice.** Any notice to the other party pursuant to this Agreement shall be deemed provided if sent by first class United States mail, postage prepaid, or by email, as follows:

To Covered Entity: Privacy Officer ("PO")
Dee Chouinard
93 Worcester Street
Wellesley, MA 02481
Dee_Chouinard@hphc.org

or to	Information Security Officer ("ISO") Ken Patterson 93 Worcester Street Wellesley, MA 02481 Ken_Patterson@hphc.org
To Business Associate:	At Broker's address on file or Broker's email address on file

The above addresses may be changed by giving notice of such change in the manner provided above for giving notice.

5.9 **Effect on Arrangement.** The provisions of this Agreement shall prevail over any provisions of the Arrangement that conflict with or are inconsistent with any provision of this Agreement. All other terms of the Arrangement shall remain in full force and effect.

5.10 **Interpretation.** This Agreement and the Arrangement shall be interpreted as broadly as necessary to implement and comply with the Privacy and Security Rule. The Parties agree that any ambiguity in this Agreement or the Arrangement shall be resolved in favor of a meaning that complies with and is consistent with the Privacy Rule.

5.11 **Costs.** Each Party, at its own expense, shall provide and maintain the personnel, equipment, hardware, software, services (including without limitation telecommunications services) and testing necessary to comply with the privacy and security provisions of this Agreement.

5.12 **Best Practices.** Attached hereto for BA's use is HPHC's Practices for Information Security.

IN Witness Whereof, the Parties hereto have duly executed the Agreement.

HARVARD PILGRIM HEALTH CARE, INC.	**BUSINESS ASSOCIATE**
By: 	By:_____
Name: Vincent Capozzi	Name:_____
Title: Senior Vice President Sales and Marketing	Title:_____
Date:_____	Date:_____

ATTACHMENT

Harvard Pilgrim Health Care
Practices for Information Security

Harvard Pilgrim Health Care is committed to the security of our members' Electronic Protected Health Information (EPHI) and Personal Information (PI). We adhere to the following security safeguards, and present these baseline practices to our Business Associates and other business partners and third parties as examples of good security practice. Our commitment to security is not only good for our healthcare members and our workforce, but makes a statement that effective, ongoing processes for maintaining information security are vital for the entire healthcare industry. We encourage our Business Associates, third parties and other business partners to join Harvard Pilgrim in following our recommendations to promote a secure information technology environment.

1. **Security Management** encompasses the policies and procedures to safeguard the confidentiality, integrity, and availability of Electronic Protected Health Information (EPHI) and Personal Information (PI), the use of tools to identify threats and vulnerabilities, escalation of security incidents that threaten the privacy of EPHI and PI, notification when a breach of privacy occurs, and ensuring compliance with the following standards:

   1.1. Complete a thorough assessment of the potential risk and vulnerabilities to the confidentiality, integrity, and availability of EPHI and PI. Implement processes, procedures, and other security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

   1.2. Perform a regular records review of information system activity (e.g., audit logs, access reports and security incident tracking reports).

   1.3. Identify a security official who is responsible for the development and implementation of the policies and procedures in place to protect the security of EPHI and PI. Harvard Pilgrim's Information Security Officer is Ken Patterson. For questions about Harvard Pilgrim's security policies or any of the best practices outlined in this document, please contact Ken at (617) 509-3068.

   1.4. Implement policies, processes, and procedures to ensure that all members of the workforce have appropriate access to EPHI and PI, and to prevent those workforce members who should not have access from obtaining access to EPHI. Implement policies and procedures for authorizing access to EPHI and PI.

   1.5. Implement procedures for the authorization and/or supervision of workforce members who will work with EPHI and PI, or in a location where EPHI or PI might be accessed.

   1.6. Implement procedures for terminating access to EPHI and PI when the employment of a workforce member ends or when there is a job change.

1.7. Implement procedures to corroborate the identity of an individual before granting access to EPHI or PI.

1.8. Implement procedures for creating, changing, and safeguarding passwords. Implement a Password Policy that includes: password minimum length, password composition, handling of unsuccessful password attempts, password re-use, preventing use of easily guessed passwords, password storage and password transmission. It is important that the Password Policy is documented and communicated throughout the organization.

1.9. Protect against malicious code, whereby hosts are updated with service packs, security vulnerability patches, virus protection, etc, in a manner appropriate to risk.

1.10. Have a security incident response plan in place that addresses the handling of a security breach, event escalation, notification, and management process, and perform a periodic test of the plan.

1.11. In the case of a security incident where the privacy of EPHI to PI is breached, notification to the covered entity or other applicable business partners or third parties should be made within twenty-four (24) hours, or one (1) business day, as to the cause and remedial steps taken to resolve the incident.

1.12. Conduct criminal background checks on workforce members who have access to EPHI or PI.

1.13. Implement sanctions for non-compliance with security policies and procedures.

1.14. Implement monitoring to perform security patch assessment, network and database security, and the review of firewall logs.

1.15. Secure all EPHI and PI transmitted via a public network or transmitted wirelessly against unauthorized access through encryption. Encrypt all PHI and PI stored on laptops or other portable devices.

1.16. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example fire, vandalism, system failure and natural disaster) that damages systems containing EPHI or PI.

1.17. Implement security awareness and training program for all workforce members, including management. At a minimum, conduct formal security training every two (2) years.

1.18. Take reasonable steps to verify that business associates and third-party service providers with access to EPHI or PI have the capacity to protect such information and contractually requiring business associates and third-party service providers to maintain such safeguards.

1.9. Document a Written Information Security Program (WISP) and update the WISP at least annually or when a change to the security program occurs.

2. **Physical Security** encompasses the policies and procedures designed to limit the physical access to EPHI, PI, and the facilities in which it is housed, the tools to identify vulnerabilities and ensure compliance to standards, and staffing to review reports and logs.

2.1. Take steps to ensure physical access controls are in place to secure access to the location, computer room(s), computer equipment, data, and paper files.

2.2. Implement physical safeguards for all workstations that access EPHI or PI, and restrict access to authorized users.

2.3. Implement procedures that document the following areas of physical security: granting access to authorized personnel, revocation of terminated workforce member's access, the escort of non-workforce members in areas where EPHI pr PI is created, received, maintained or transmitted, and safeguarding the storage of paper files.

2.4. Implement procedures to address the following areas: safeguarding the storage of tape backups, logs, mail messages and other electronic media containing EPHI or PI.

2.5. Implement policies and procedures to address the final disposition of EPHI, PI, and/or the hardware of electronic media on which it is stored.

3. **Network And Audit Security Vulnerability Assessment** is performed as a safeguard to help verify that software patch and network configurations are secure against known threats. Security of its network configuration should be verified through the following:

3.1. Contract with an independent third party to perform a network security assessment on server(s) and network perimeter.

3.2. Review the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonable implicate the security or integrity of records containing EPHI or PI.