### Certification of Compliance with HIPAA Privacy Rule

WHEREAS \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (“Plan Sponsor”) is the sponsor of an employee welfare benefit plan for its employees and their dependents; and

WHEREAS Plan Sponsor’s employee welfare benefit plan includes a group health plan (“Group Health Plan”) within the meaning of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”); and

WHEREAS Harvard Pilgrim Health Care (“Harvard Pilgrim”) provides health insurance coverage to the participants and beneficiaries in the Plan Sponsor’s Group Health Plan; and

WHEREAS Harvard Pilgrim, Group Health Plan, Plan Sponsor, and third-party designees desire to exchange health information protected under HIPAA (protected health information and electronic protected health information [EPHI], collectively referred to herein as “PHI”) for purposes related to administration of the Group Health Plan.

Plan Sponsor hereby certifies to Group Health Plan and to Harvard Pilgrim, as required by 45 CFR Sections 164.314(b) and 164.504(f) of HIPAA, that Plan Sponsor agrees to:

* Not use or further disclose PHI other than as permitted or required by the plan documents or by law;
* Ensure that any agents, including subcontractors, to whom it provides PHI received from Group Health Plan or Harvard Pilgrim agree to the same restrictions and conditions that apply to Plan Sponsor with respect to such information;
* Not use or disclose PHI for employment-related actions and decisions;
* Not use or disclose PHI in connection with any other benefit or employee benefit plan of Plan Sponsor;
* Report to Harvard Pilgrim any use or disclosure of PHI that it becomes aware of which is inconsistent with the uses or disclosures provided for;
* Make PHI available to an individual based on HIPAA’s access requirements;
* Make PHI available for amendment and incorporate any PHI amendments based on HIPAA’s amendment requirements;
* Make available the information required to provide an accounting of disclosures;
* Make its internal practices, books and records relating to the use and disclosure of PHI received from Group Health Plan or Harvard Pilgrim available to the Secretary of the U.S. Department of Health and Human Services to determine the Group Health Plan’s compliance with HIPAA;
* Ensure that adequate separation between Group Health Plan and the Plan Sponsor is established as required by HIPAA (45 CFR 164.504(f)(2)(iii) and that such separation is supported by reasonable and appropriate security measures;
* If feasible, return or destroy all PHI received from Group Health Plan or Harvard Pilgrim that Plan Sponsor still maintains in any form and retain no copies of such PHI when no longer needed for the specified disclosure purpose. If return or destruction is not feasible, Plan Sponsor will limit further uses and disclosures to those purposes that make the return or destruction infeasible;
* Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the EPHI that it creates, receives, maintains, or transmits on behalf of Group Health Plan or Harvard Pilgrim;
* Identify those Group Health Plan Staff that have access to PHI;
* Ensure that any agent, including a subcontractor, to whom it provides EPHI agrees to implement reasonable and appropriate security measures to protect the information; and
* Report to Group Health Plan and Harvard Pilgrim any breach of security of which it becomes aware that results in the unauthorized access, use, disclosure, modification or destruction of PHI

The reverse side of this page contains Harvard Pilgrim’s Policy for Disclosure of Member Information. Signature below indicates Plan Sponsor’s receipt and understanding of this Policy.

Signature (Plan Sponsor) Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Print name Title

**Harvard Pilgrim Health Care**

**Policy for Disclosure of Member Information**

Harvard Pilgrim Health Care (HPHC) reviews all requested disclosures to ensure compliance with its corporate policies, the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, and all other federal and state laws addressing privacy and security.

Each request for Protected Health Information (PHI), including data in certain categories identified in federal and state laws not otherwise codified within HIPAA’s Privacy Rule (“protected category information”), is reviewed to validate the disclosure is necessary to meet the stated and legitimate business purpose.

HPHC uses the phrase ‘protected categories’ to refer to sensitive diagnoses, procedures or treatments such as those exclusively associated with HIV/AIDS, abortion, genetic testing, and substance abuse (federal law limits the use of substance abuse information to audits or program evaluations). HPHC implements safeguards regarding the disclosure of specific data elements that reveal the prior, current or possible future health status of an individual, and to which federal and/or state governments have afforded additional protections. These protections are more specific regarding certain categories of clinical care and conditions than the general, non-specific definition of PHI contained within the Privacy Rule.

Self-funded Group Health Plans, and fully-funded Group Health Plans certifying HIPAA compliance, are considered “Covered Entities” according to the Privacy Rule, and, like HPHC, must comply with the provisions set forth in the Rule related to the safeguarding of PHI.

HPHC prefers to exclude protected category information from extracts/reports or, alternatively, provide such information without individual identifiers. If it is determined that protected category information is required by the Group Health Plan for a legitimate business purpose, HPHC may include such data providing the Group Health Plan has met all HIPAA privacy and security requirements.

The signature of the Plan Sponsor (on the reverse side of this page) indicates compliance with HIPAA’s Privacy and Security Rules and understanding of the Plan Sponsor’s obligation to comply with applicable state and federal laws with regard to PHI.