I Purpose

Harvard Pilgrim Health Care (Harvard Pilgrim) values its members’ privacy rights and is committed to safeguarding protected health information (PHI). To support this commitment, Harvard Pilgrim has taken reasonable steps to use or disclose only the minimum amount of PHI necessary for treatment, payment, or health care operations (TPO) as required under applicable federal, state, and/or local regulations. This policy provides an overview of the policies Harvard Pilgrim has implemented for the use and disclosure of PHI.

II Policy

• Harvard Pilgrim will implement policies and procedures related to the uses and disclosures of information in a manner that safeguards the privacy rights of its members’ PHI in accordance with federal, state, and/or local regulations. PHI may be used and/or disclosed as necessary for treatment, payment, or health care operations. PHI may also be used or disclosed when authorized by the member, his/her designated personal representative, for research studies where authorization has been waived by Harvard Pilgrim’s Institutional Review Board (IRB), or when permitted or required by law. Permitted uses/disclosures are outlined in Harvard Pilgrim’s Notice of Privacy Practices.

• Harvard Pilgrim staff will use/disclose only the minimum necessary amount of PHI when responding to requests.

• The use, access and/or disclosure of PHI related to Harvard Pilgrim employees who are subscribers of the Harvard Pilgrim Group Health Plan is further restricted. PHI will be used for the administration (e.g., enrollment, billing) of the Group Health Plan. Appropriate safeguards are in place to protect against its use for employment-related decisions. Harvard Pilgrim has a responsibility to safeguard this information and fulfills this responsibility by limiting the use and access of this PHI to only certain members of its workforce. (See Safeguarding GHP Data Policy.)

Note: Employees who are dependents of subscribers of Group Health Plans other than Harvard Pilgrim, are subject to the general (not the “employee as member”) privacy rights outlined within this policy.

• This policy applies to Harvard Pilgrim’s workforce and the business associates that contract with Harvard Pilgrim to provide services on its behalf.

All members of Harvard Pilgrim’s workforce are required to complete training on HIPAA’s Administrative Simplification Rules. Workforce members will receive retraining within 30 days after a material change in their job function has occurred. (See Workforce Training Policy.)

• The Safeguarding of PHI Policy and related policies must be reviewed and the review acknowledged in writing at the time an employee begins employment with Harvard Pilgrim. Each employee will be required to attest to the review of these policies on an annual basis thereafter. The Safeguarding of PHI Policy and all associated policies set forth Harvard Pilgrim’s expectations for all workforce members regarding the procedures that must be followed to safeguard the privacy and security of member information. Any employee who violates this policy is subject to disciplinary action, up to and including termination. (See Corporate Sanction Policy.)

III Procedures

Use & Disclosure

• VERIFICATION: Prior to disclosing PHI, Harvard Pilgrim staff will take reasonable steps to verify the identity of the person requesting the information, and the authority of the person to access the PHI. (See Verification Policy.)

• DESIGNATED PERSONAL REPRESENTATIVE: In the event that a member wishes to designate someone else to make decisions related to his/her health care, the member must have written documentation on file at Harvard Pilgrim designating this individual to act on his/her behalf. (See Designation of Personal Representative Policy.)

• PERMITTED DISCLOSURES: Harvard Pilgrim is permitted to use and disclose PHI, with individual authorization, or in the following circumstances, without individual authorization:
  - When the disclosure is to the individual to whom the PHI pertains.
  - For TPO, also known as “routine disclosures.”
  - Between covered entities which have a relationship with the individual.
  - In compliance with the Designation of a Personal Representative Policy.
  - To conduct formal research studies that have been reviewed by an IRB, and for which the authorization requirements have been waived.
MEMBER CARE—PROTECTING HEALTH INFORMATION
Safeguarding of Protected Health Information (cont.)

MEMBER CARE—PROTECTING HEALTH INFORMATION
Safeguarding of Protected Health Information (cont.)

- When requested by the Secretary of Health and Human Services (HHS) to investigate Harvard Pilgrim’s compliance with Privacy Rule standards. (See Disclosure of PHI Policy.)
In addition to the permitted disclosures above, the following disclosures do not require an authorization:
- Disclosures about victims of abuse, neglect, or domestic violence.
- Uses or disclosures for public health activities.
- Uses or disclosures for health oversight activities to a health oversight agency.
- Disclosures for judicial and administrative proceedings.
- Disclosures for law enforcement purposes. (See Authorization Policy.)

• UNDERWRITING: At times, Harvard Pilgrim Health Care will receive and use demographic, aggregate claims experience, and individual large claims information about prospective members to evaluate likely future claims experience and to set appropriate rates. This information is subject to all protections afforded to the health information of Harvard Pilgrim members including, but not limited to, use and disclosure procedures, minimum necessary guidelines, and physical and technical safeguards.

• MEMBER AUTHORIZATION: Harvard Pilgrim will obtain a written authorization from the member about whom it is requesting/making a disclosure in order to obtain/disclose PHI for non-TPO purposes, or for purposes not otherwise permitted by law. In addition, there is a separate policy describing the process Harvard Pilgrim will use to determine if certain member communications are considered marketing as described by HIPAA’s Privacy Rule (Marketing policy and filter.) In some cases, member authorization will be required. (See Member Authorization Policy.)

There are certain instances when oral authorization meets the HIPAA requirement, such as disclosures to family/friends who are involved in an individual’s care. In these instances, disclosures of PHI are permitted without written authorization, provided that the member has an opportunity to agree, prohibit, or restrict the disclosure in advance. Harvard Pilgrim’s staff may obtain oral agreement from the member only after the identity of the member has been verified.

• MINIMUM NECESSARY: When using, disclosing, or requesting PHI, Harvard Pilgrim will make reasonable efforts to limit PHI to the minimum necessary amount to accomplish the intended purpose. Minimum necessary does not apply to:
  - Disclosures to, or requests by, a health care provider for treatment purposes;
  - Uses or disclosures made to the individual who is the subject of the PHI, or to his/her designated personal representative;
  - Uses or disclosures made pursuant to an authorization, unless the authorization itself limits the amount of PHI to be released;
  - Disclosures made to the Department of Health and Human Services (DHHS), or uses/disclosures required for compliance;
  - Uses or disclosures that are required by law. (See Minimum Necessary Policy.)

• ROLE-BASED ACCESS: In order to carry out their job responsibilities, members of Harvard Pilgrim’s workforce and others may access PHI. Harvard Pilgrim has made reasonable efforts to safeguard PHI by limiting access to PHI based on documented job functions and/or responsibilities. (See Role-Based Access Policy.)

• DE-IDENTIFICATION/LIMITED DATA SET: Data that has been de-identified, is not considered PHI and is not subject to this policy. Harvard Pilgrim may, for this purpose, use standardized methodology to create information that is not individually identifiable health information. Harvard Pilgrim may determine that information is de-identified when all eighteen elements of PHI are removed. (See De-identification Policy.)

Additionally, a Limited Data Set may be utilized for the purposes of research, public health, or health care operations if an appropriate Data Use Agreement is in place. Data in a Limited Data Set is considered PHI and is subject to the safeguards outlined in this policy. (See Limited Data Set Policy.)

Patient Rights

• NOTICE OF PRIVACY PRACTICES: Harvard Pilgrim has a responsibility to inform members of the permitted uses and disclosures of PHI, an individual’s rights under the HIPAA Privacy Rule, and Harvard Pilgrim’s legal responsibilities with respect to PHI. Harvard Pilgrim’s Notice of Privacy Practice outlines each of these components and is provided to all current subscribers, and to new subscribers upon enrollment in the Plan. The Notice is also available upon request and posted on Harvard Pilgrim’s Web site. (See Privacy Notice Policy.)

The individual rights detailed in the Notice of Privacy Practice include member rights to:

• Inspect, amend, and obtain a copy of their PHI as part of a Designated Record Set (determined via the Members’ Rights to Access, Inspect, and Obtain a Copy of Protected Health Information Policy, for as long as that PHI is maintained in the Designated Record Set request restrictions to use/disclose their PHI. (See Right to Restrict Access Policy.)

• Request an alternate means of communication. (See Member Right to Request Confidential Communications Policy.)

• Voice a complaint using the complaint process if he/she feels his/her privacy rights have been violated. (See Member Complaint Policy.)

(continued)
Business Associates

- **BUSINESS ASSOCIATE AGREEMENTS**: At times, Harvard Pilgrim may contract with other organizations to provide services on its behalf. As these services, functions, or activities are performed, PHI may be accessed or disclosed. Examples of Business Associates include: consultants, accountants, behavioral health management companies, and pharmacy benefit managers. In these cases, Harvard Pilgrim will enter into an agreement explicitly outlining the requirements associated with the use and disclosure of PHI. *(Business Associate Agreement)* as mandated by the HIPAA Privacy Rule. *(See Business Associate Policy)*

Safeguards

- **PHYSICAL SAFEGUARDS**: Within Harvard Pilgrim, PHI is stored in a secure location, e.g., locked files, to which access is limited to authorized Harvard Pilgrim workforce members. Access to the building and/or specific floors within a mixed occupancy facility is restricted to those with the appropriate Access Cards and/or monitored by Security personnel at the entrances of the buildings. *(See Access and ID Cards Policy)*
- **FAX**: The transmission of PHI via facsimile (fax) is permitted provided that a Standard Cover Sheet, containing confidentiality language, is used, the sender ensures that an appropriate person is available to receive the fax as it arrives, and that the fax is being sent to a secure location. *(See Sending and Receiving Facsimiles Policy)*
- **TECHNICAL SAFEGUARDS**: Harvard Pilgrim maintains technical security policies and procedures relating to electronic storage, maintenance, and transmittal of PHI, including authentication requirements, password controls, audit trails, email encryption, and Internet use.
- **E-MAIL**: PHI may not be included in an electronically transmitted message over a public network, i.e., Internet, except as permitted by and in accordance with the Harvard Pilgrim e-mail policy. Files containing PHI may be sent over public networks only if the document has been encrypted using approved controls. *(See Corporate E-mail Policy)*
- **WORKSPACE/PUBLIC AREAS**: PHI should never be discussed in public areas, including but not limited to hallways, elevators, restrooms, and cafeterias. When discussing PHI in a workspace, workforce members must be particularly cognizant of the sensitive nature of the information and use reasonable safeguards to protect PHI. Although incidental exposure will sometimes occur, it is the responsibility of every member of the workforce to safeguard against incidental disclosure of PHI. *(See Safeguarding of PHI in the Workspace Policy)*
- **DISPOSAL OF PHI**: When no longer needed or required by law, PHI will be properly disposed of, or destroyed, so that it is unrecoverable. Receptacles are located throughout each facility for proper paper disposal of PHI including bins for shredding. In addition, members’ PHI on electronic media will be disposed of in accordance with Harvard Pilgrim’s Policy on the Disposal of Computer Magnetic Storage Media. *(See Disposal/Destruction of Confidential Policy)*

Administration & Enforcement

- **MITIGATION**: Harvard Pilgrim maintains policies and procedures to mitigate harmful effects in the event of a violation of this policy or an improper use/disclosure of PHI. *(See Mitigation Policy)*
- **PRIVACY OFFICER**: Harvard Pilgrim has designated a Privacy Officer who has oversight responsibility for the development and implementation of privacy policies and procedures in order to comply with the HIPAA Privacy Rule. *(See Designation and Responsibilities of the HPHC Privacy Officer Policy)*
- **INFORMATION SECURITY OFFICER**: Harvard Pilgrim has designated an Information Security Officer who has responsibility to oversee development and enforcement of security policies and procedures in order to comply with the HIPAA Privacy & Security Rules.
- **REFRAIN FROM RETALIATION**: Harvard Pilgrim will refrain from retaliatory actions against individuals (members, employees, etc.) for reporting a suspected incident of non-compliance, breach of privacy, or for filing a complaint against another individual who is or may be non-compliant with the standards set forth in this policy. *(See Non-Retalialatory Action Policy)*
- **EMPLOYEE SANCTIONS**: This *Safeguarding of PHI Policy* and related policies must be reviewed and the review acknowledged in writing at the time an employee begins employment with Harvard Pilgrim. Each employee will be required to attest to the review of these policies on an annual basis thereafter. *The Safeguarding of PHI Policy* and all associated policies set forth Harvard Pilgrim's expectations for all workforce members regarding the procedures that must be followed to safeguard the privacy of member information. Any employee who violates this policy is subject to disciplinary action, up to and including termination. *(See Sanction Policy)*

Other

- **FUNDRAISING**: As a matter of corporate policy, Harvard Pilgrim does not use or disclose PHI for fundraising activities. In the future, should Harvard Pilgrim plan to use or disclose demographic information for fundraising, an opt-out procedure will be designed and implemented in accordance with the Rule.

This policy will be reviewed on an annual basis.