MAPFRE U.S.A. CORP.
Health Plans and Health Flexible Spending Account
HIPAA Privacy Policy

Introduction

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and regulations implementing the medical privacy provisions of HIPAA (the "Privacy Rule") restrict the ability of certain entities, referred to as Covered Entities, to use and disclose protected health information. While MAPFRE U.S.A. Corp. ("Company") is not a "Covered Entity" directly subject to the Privacy Rule, the MAPFRE U.S.A. Corp. Health Flexible Spending Account and MAPFRE U.S.A. Corp. Health Plans are subject to the Privacy Rule.

HIPAA requires that the Plans meet certain administrative requirements and adopt certain policies and procedures to insure the privacy of protected health information ("PHI"). It is the policy of Company and the Plans to comply fully with HIPAA's requirements. Accordingly, Company, as sponsor of the Plans, adopts this Privacy Policy on behalf of itself and on behalf of the Plans.

I. Overview and Scope

This policy applies with respect to PHI received, maintained, used or disclosed by representatives of the Plans. For purposes of this policy, "PHI" is information, created or received by the Plans, that relates to the past, present, or future physical or mental health or condition of an individual; to the provision of health care to an individual; or to the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or for which there is a reasonable basis to believe the information can be used to identify the individual. PHI includes information of persons living or deceased. A use or disclosure of PHI is permitted only to the extent such use or disclosure is consistent with the Privacy Rule and this policy.

This policy does not apply directly to personal information, including medical information, that employees or agents of Company may receive, maintain, use or disclose in Company's capacity as employer, although such information is subject to Company's general privacy and confidentiality policies, and the handling and use of this information may be restricted by other state or Federal law. Accordingly, it is Company's policy that any personal information concerning a Company employee or family member of a Company employee will be handled in a manner that respects the personal and confidential nature of that information; the procedures in this policy are instructive in that regard.

The effective date (the "Effective Date") of this policy is April 14, 2003. This policy has been most recently amended and restated as of January 1, 2015. The person charged with administering this policy is the "Privacy Official," Jose Luis Velasquez Vigil, Executive Vice President, Human Resources.

II. Access to PHI

A. Company Employees. Access to PHI is limited to the following categories of employees who may come into contact with PHI in the course of their duties at Company:

- Employees that support the Benefits Function
- Employees that support the HR Function
- Employees that support the Treasury Function
- Employees that support information technology

Notwithstanding the foregoing restrictions, any employee who in fact accesses PHI shall be subject to this policy, whether or not the access is contemplated by this policy.

B. Business Associates. Agents or contractors of Company who perform services with respect to the Plans may also access PHI in the course of performing plan administrative functions or in the course of advising Company with respect to the Plans. Any such agent or contractor shall be termed a "business associate" of the Plans. PHI may not be shared with a business associate unless a Business Associate Agreement is in place on or before the Effective Date, or at such later time and under such conditions as may be permitted by the Privacy Rule.

III. Permitted Uses and Disclosures

The following uses and disclosures of PHI may be made by, between and among the Company employees described in Section IIA and the Plans' business associates (and their employees and agents). The Plans shall be amended to permit these disclosures from the Plans to Company, and Company (in its capacity as plan sponsor) shall so certify to the Plans as required by the Privacy Rule.

A. Plan Administration. PHI may be used or disclosed for the Plans' administrative functions, but only to the extent the use or disclosure is limited to the minimum amount necessary to perform the Plans' administrative function. The Plans' administrative functions include treatment, payment and health care operations.

- **For Payment**. PHI may be used and disclosed in order to determine eligibility for Plan benefits, to facilitate payment for treatment and services, to determine benefit responsibility under the Plans, or to coordinate Plan coverage. For example, a Plan's third party administrator ("TPA") may use PHI to process a claim for reimbursement and make a determination as to whether the service is covered by the Plans. As another example, a TPA may also access PHI in order to mail Explanation of Benefits forms and other information to the primary subscriber (the Company employee or former employee).
- **For Health Care Operations**. The Plans may use and disclose PHI for other Plan operations that are deemed necessary to administer the Plans. For example, Company employees or business associates (such as payroll vendors or TPAs) may access certain information as part of the enrollment process. The Plans may use PHI in connection with: conducting quality assessment and improvement activities; underwriting, premium rating, and other activities relating to Plan coverage; submitting claims for stop-loss (or excess loss) coverage; conducting or

arranging for medical review, legal services, audit services, and fraud and abuse detection programs; business planning and development such as cost management; and business management and general Plan administrative activities.

- **For Treatment**. In certain circumstances, the Plans may use or disclose PHI in order to facilitate medical treatment or services by providers. For example, it may be necessary to pre-certify that a given service or procedure is covered by a Plan.

B. Pursuant to an individual's authorization. PHI may be used or disclosed pursuant to and consistent with a participant's authorization, including an employee's authorization to release information to Company. A copy of the individual's authorization shall be provided to the Privacy Official.

C. For government oversight and public policy. PHI may be disclosed for purposes of a governmental audit of the Plans' HIPAA compliance. In addition, with approval of the Privacy Official (which may be done on a case-by-case or general basis), PHI may be disclosed: 1) for public health and welfare purposes, such as public health and safety, abuse and neglect matter or threats to security; 2) for health oversight activities, such as the Food and Drug Administration, the Department of Labor, or applicable state regulators; 3) in connection with organ and tissue donation; 4) to coordinate benefits; and 5) to comply with Worker's Compensation or similar law. The Privacy Official shall be notified of any such disclosures.

D. To the individual. PHI may be disclosed to the participant pursuant to an exercise of his or her individual HIPAA rights.

IV. Disclosures to Employer are Limited

PHI may not be used or disclosed by the Plans for the payment or operations of Company's "non-group health" benefits (e.g., disability, life insurance, etc.), or for purposes of an employment action by Company, unless the participant has provided an authorization for such use or disclosure, or such use or disclosure is required by applicable state law and particular requirements under HIPAA are met.

V. Exercise of Individual Rights

The Plans provide that participants have certain rights and access to information. Participants requesting access to or the exercise of other rights with respect to the PHI maintained by the Plans must make a request in writing to the TPA, on such form as the TPA may require. The TPA shall respond to the request within a reasonable period of time, taking into account the nature of the request. If the TPA fails to respond within 30 days of the initial request, the participant may institute a request for review by notifying the Privacy Official. The Privacy Official shall monitor the TPA's administration of individual rights requests to ensure that the Privacy Rule is being implemented.

Determinations on behalf of the Plans with respect to the exercise of individual rights shall initially be made by the TPA. If a participant is not satisfied with the determination made by the TPA, the participant may request that the Privacy Official review the initial determination, and may then institute a claim under the Plans' claim procedures.

As of the Effective Date, the contact address for instituting the exercise of the following individual rights is MAPFRE U.S.A. Corp., Attn: Jose Luis Velasquez Vigil, 11 Gore Road, Webster, MA 01570. Participants should be referred to that address in order to institute an exercise of individual rights.

A. Access to Protected Health Information and Requests for Amendment

A plan participant may request access to and obtain copies of his or her PHI that is maintained in "designated record sets" by a Plan or one of its business associates. The Plans will provide access to and copies of a participant's PHI pursuant to requests that are submitted in writing by participants. The Plans may charge a fee for the costs of copying, mailing or other supplies associated with the request. The Plans may deny the request only as provided in the Privacy Rule.

B. Right to Request Restrictions

A participant has the right to request a restriction or limitation on the medical information the Plans use or disclose for treatment, payment or health care operations. A participant may also request a limit on the medical information that the Plans disclose to someone who is involved in the participant's care or the payment for the care, like a family member or friend. The Plans, through the TPA and the Privacy Official, have full discretion in making the determination as to whether the Plans will agree to the request, but if a Plan does agree, the Plan will put any limits in writing and follow such unless an emergency situation arises. The TPA shall ensure that its personnel are informed of and comply with the limits, and shall inform the Privacy Official of any such restrictions.

C. Right to Amend

Participants may request that the PHI maintained by the Plans be amended or corrected. The Plans may deny a participant's request if it makes a determination that the requested amendment:

- is not part of the medical information kept by or for the Plans;
- was not created by the Plans, unless the person or entity that created the information is no longer available to make the amendment;
- is not part of the information which the participant would be permitted to inspect and copy; or
- is accurate and complete.

D. Right to a List or Accounting of Disclosures the Plans Have Made

A participant has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years (but not prior to the Effective Date), other than disclosures made (i) to carry out treatment, payment or health care operations; (ii) to individuals about their own PHI; (iii) incident to an otherwise permitted use or disclosure; (iv) pursuant to an authorization; (v) for purposes of creation of a facility directory or to persons involved in the patient's care or other notification purposes; (vi) as part of a limited data set; or (vii) for other national security or law enforcement purposes. The accounting must include the date of the disclosure, the name of the receiving party, a brief

description of the information disclosed, and a brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any). The first accounting in any 12-month period shall be provided free of charge. The Privacy Official may impose reasonable production and mailing costs for subsequent accountings, and will notify the participant of the cost to be borne by the Participant before the costs are incurred.

A Plan shall respond to an accounting request within 60 days. If a Plan is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the participant notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.

E. Right to Request Confidential Communications

A participant may request that the Plans communicate about medical matters in a certain way or at a certain location such as using an alternate address or through a specific format such as e-mail. The Plans have the sole discretion to determine whether to honor such requests, although it is the intent to accommodate all reasonable requests.

VI. Communication with Participants

A. Authorized representatives. Except in emergency situations, or as otherwise permitted by this procedure, the Plans will disclose an individual's PHI only to the individual or his or her authorized representative. The Plans may implement authorization forms allowing PHI with respect to a subscriber or any person receiving Plans coverage through the subscriber to be shared with the subscriber and/or his or her spouse or domestic partner. The Plans may treat either the employee or non-employee parent of a minor child as authorized to receive PHI, unless the Plans has on record a court order or other documentation limiting disclosures to one or both parents.

B. Verifying identity. Representatives of the Plans, including business associates, shall implement an authentication or verification process when speaking with a participant or a participant's representative about a participant's PHI. For example, a phone representative may request a subscriber number or other individually identifying information, before speaking with an individual about an individual's PHI.

C. Mailings. The Plans will send all written communication concerning a subscriber or any person receiving Plans coverage through the subscriber to the address on file for the subscriber unless an individual requests another means of communication.

VII. Technical and Physical Safeguards

Plan representatives, including Company employees, shall adopt appropriate technical and physical safeguards that will prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements, including the "minimum necessary" requirement. Accordingly, communications regarding PHI should be undertaken in a manner that preserves the confidentiality of the information. If the identity of the individual about whom health information is used or disclosed is not necessary for the use or disclosure, the identity and all identifying information shall be protected. PHI shall be discarded or deleted once the purpose for which it is obtained has been completed, although nothing in this policy shall preclude the

preservation of PHI as may be necessary to defend against a claim made against the Plans, Company or a business associate.

In addition, Plan representatives shall generally observe the following specific confidentiality procedures with respect to PHI: (1) PHI shall be maintained in a manner that is separate from health information that Company may maintain for other reasons (such as administration of Company's FMLA policy or LTD plan); (2) access to paper or electronic files containing PHI shall be limited; (3) email communication concerning PHI shall be conducted in a manner that insures the email is not available to personnel who do not need to access the email as part of their job function; (4) verbal communication concerning PHI shall be limited; and (5) processes for verifying the recipient of facsimile communications shall be implemented.

VIII. Breach of Unsecured PHI

A. General. The Company handles protected health information of its employees in connection with the Company's administration of the self-insured portion of its health insurance benefit.

B. Definitions. A breach is the acquisition, use or disclosure of unsecured PHI in a manner not permitted by HIPAA's Privacy Rule that compromises the security or privacy of the unsecured PHI. PHI is unsecured if it is not rendered unusable, unreadable or indecipherable to unauthorized individuals through encryption, destruction or other means.

C. Presumed breach. Except as provided below in paragraph D, an acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule is presumed to be a breach unless Plan demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

D. Exceptions. A breach does not include (i) any unintentional acquisition, access, or use of PHI by a Company employee authorized to access PHI or by a person acting under the authority of such employee or a Business Associate, if it was made in good faith and within the scope of authority, and does not result in further use or disclosure in a manner not permitted under the Privacy Rule; (ii) any inadvertent disclosure by such employee or a Business Associate who is authorized to access PHI, to another person authorized to access PHI at the Company or the Business Associate, so long as the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule; or (iii) a disclosure of PHI where the authorized employee or a Business Associate has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

E. Obligation to report suspected or actual breaches. Any employee or representative of the Company who becomes aware of an actual or suspected Breach must immediately notify the Privacy Official in writing via email at JVelasquezVigil@mapfreusa.com or via telephone at (508) 949-4995 within four (4) hours immediately after the employee suspects or becomes aware of such potential breach or misuse. The Privacy Official will instruct the employee if any additional steps need to be taken.

1. Investigation required upon report of a suspected or actual breach. The Privacy Official shall immediately undertake an investigation to determine if the unauthorized use or disclosure constitutes a Breach under the Privacy Rule. All such investigations shall be documented.
2. Notification to Participants. If notification to participants is legally required, the Privacy Official, or its designee, will notify in writing each participant whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed, as soon as possible after the discovery of such Breach (but under no circumstances later than 60 days after the discovery of the Breach or, to the extent feasible, any earlier date that the Breach should have been discovered through the exercise of reasonable diligence). In the event of a Breach by a Business Associate, the Privacy Official may, if the Business Associate or the Business Associate Agreement allows, work with the Business Associate to ensure that the Business Associate undertakes notification on behalf of the Plan in the manner required by the Privacy Rule, at expense of the Business Associate.
3. Written Notification. Any written notice of Breach is to be sent by first class mail to the participant's last known address, or if there is valid authorization from the participant to receive notice by email, then by email. In the event there is out-of-date contact information that precludes written notice, then the Plan shall use an alternative form of notice reasonably calculated to reach the participant.
4. Urgent Notifications to Participants. In any case deemed by the Plan to require urgency because of possible imminent misuse of a participant's Unsecured PHI, then the participant must also be contacted as soon as possible by telephone or by other means, as appropriate, in addition to the notification noted above.

5. Content of Notification to Participants. The notice to participants will include, to the extent possible: (1) a brief description of what happened, including the date of the Breach and the date of its discovery, if known; (2) the type of Unsecured PHI involved in the Breach; (3) the steps the participant should take to protect him/herself; (4) what the Plan is doing to investigate the Breach, mitigate harm, and protect against further breaches; and (5) contact procedures the participant can use to ask questions or learn additional information, which shall include an email address, toll-free telephone number, website address or postal address.

6. Notifications to HHS. If a Breach affects 500 or more participants, then at the same time the notification requirements above are satisfied, the Privacy Official shall notify HHS electronically and in the manner specified on the HHS website by filling out the form at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html. In the event of a Breach by a Business Associate, the Plan will determine in each instance whether the requisite notice will be provided by the Plan or by the Business Associate.

7. Notifications to the Media. If a Breach affects 500 or more participants who reside in a particular state or other jurisdiction, such as a county or town, then in addition to the notice requirements described above, notice of the Breach must also be provided to prominent media outlets serving the state or jurisdiction. This notification should be made as soon as possible after the discovery of the Breach (but under no circumstances later than 60 days after the discovery of the breach or, to the extent feasible, any earlier date that the breach should have been discovered through the exercise of reasonable diligence). In the event of a Breach by a Business Associate, the Plan will determine in each instance whether this notice will be provided by the Plan or by the Business Associate.

8. Documentation of Breaches. For Breaches that affect fewer than 500 participants, the Privacy Official shall maintain a log or other documentation of such Breaches and shall, not later than 60 days after the end of each calendar year, provide HHS with notice of Breaches discovered during the preceding calendar year, in the manner specified on the HHS website and by filling out and submitting electronically the form at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html. A separate form must be completed for each Breach that was discovered during the preceding calendar year.

IX. Complaints, Violations and Self Audit

A. Identifying Violations. The Privacy Official will be the primary contact person for receiving complaints. Complaints or questions concerning the application of the Plans' privacy procedures or compliance with HIPAA may be made by a Plan participant, a Plan representative (including business associates), or any Company employee. Formal complaints shall be made in writing addressed to the Privacy Official and shall include a statement that the individual is

instituting a complaint procedure under this policy. The Privacy Official may also from time to time audit the compliance of the Plans and its business associates with this policy and the Privacy Rule. The Privacy Official shall document any investigations concerning possible violations of this policy or the Privacy Rule on the part of the Plans.

B. Correction of Violations. The Plans will promptly correct any violation of the Privacy Rule reported or known to the Privacy Official to the extent possible. If full correction is not possible, the Plans will mitigate or lessen, to the extent possible, any harmful consequences of the violation. Such correction or mitigating steps may include requesting the destruction of PHI or obtaining agreement as to the limitation on its use.

C. Sanctions. Appropriate sanctions up to and including termination of employment will be imposed upon employees who disclose PHI in violation of this policy and the Privacy Official shall document such sanctions.

X. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA. No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.

XI. Workforce Training

Company employees described in II.A. above shall be trained on and receive a copy of this privacy policy.

XII. Notice

Participants shall receive notice of the Plans' HIPAA privacy policy upon enrollment and periodically thereafter as required by the Privacy Rule.

XIII. Amendment; Implementation

The Privacy Official may amend this policy at any time for any reason, including as may be necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented, and appropriate Plan personnel (including business associates) shall be notified of the change. The Privacy Official shall have complete discretion to adopt such rules, regulations, practices or procedures as he or she deems necessary or appropriate to implement this privacy policy.