MphasiS Employee Health and Welfare Benefit Plan
HIPPA Privacy Policy

Table of Contents

A. Introduction

MphasiS (the “Company”) sponsors the MphasiS Employee Health and Welfare Benefit Plan, a self-funded group health plan (hereinafter referred to as “Plan”).

Members of the Company’s workforce may have access to protected health information (“PHI”) of Plan participants (1) on behalf of the Plan itself; or (2) on behalf of the Company, for administrative functions of the Plan and other purposes permitted by the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). HIPAA and its implementing regulations restrict the Plan’s and the Company’s ability to use and disclose Protected Health Information. Protected Health Information means information that is created or received by the Plan and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of the health care to the participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. Protected Health Information includes information of persons living or deceased. Note that the Company may also sponsor other plans that are not subject to this privacy policy, and this Privacy Policy will govern the circumstances, if any, that Plan PHI may be shared with any such other plans.

It is the Company’s policy that the Plan shall comply with HIPAA’s requirements for the privacy of PHI. To that end, all members of the Company’s workforce who have access to PHI must comply with this Privacy Policy. For purposes of this Policy and the Plan’s more detailed Privacy Use and Disclosure Procedures, the Company’s workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of the Company, whether or not they are paid by the Company. The term “employee” includes all of these types of workers.

No third-party rights (including but not limited to rights of Plan participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Policy. The Company reserves the right to amend or change this Policy at any time, either prospectively or retroactively, without notice. To the extent this Privacy Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational and shall not be binding upon the Plan or the Company. This Policy does not address requirements under other federal laws or under state laws. To the extent this Policy is in conflict with the HIPAA privacy rules, the HIPAA privacy rules shall govern.

B. Plan's Responsibilities as Covered Entity

I. Privacy Official and Contract Person

Sanju Verma AVP and Lead International HR will be the Privacy Official for the Plan. The Privacy Official will be responsible for the development and implementation of policies and procedures relating to privacy of the Plan's PHI, including but not limited to this Privacy Policy and the Plan's Privacy Use and Disclosure Procedures. The Privacy Official will also serve as the contract person for participants who have questions, concerns, or complaints about the privacy of their PHI.

The Privacy Official is responsible for ensuring that the Plan complies with the provisions of the HIPAA privacy rules regarding business associates, including the requirement that the Plan have a HIPAA-complaint Business Associate Agreement in place with all business associates. The Privacy Official shall also be responsible for monitoring compliance by all business associates with the HIPAA privacy rules and this Privacy Policy.

II. Workforce Training

It is the Company's policy to train all members of its workforce who have access to Plan PHI on the Plan's Policy and its Privacy Use and Disclosure Procedures. The Privacy Official is charged with developing training schedules and programs so that all workforce members receive the training necessary and appropriate to permit them to carry out their Plan functions in compliance with HIPAA.

III. Safeguards and Firewall

On behalf of the Plan, the Company will establish appropriate administrative, technical, and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Administrative safeguards include implementing procedures for use and disclosure of PHI. Technical safeguards include limiting access to information by creating computer firewalls, as well as physical safeguards which may include locking doors or filing cabinets.

Fire walls will ensure that only authorized employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for Plan administrative functions, and that they will not further use or disclose PHI in violation of HIPAA's privacy rules.

IV. Privacy Notice

The Privacy Official is responsible for developing and maintaining a notice of the Plan's privacy practices that describes:

- The uses and disclosures of PHI that may be made by the Plan
- The rights of individuals under HIPAA privacy rules
- The Plan's legal duties with respect to the PHI
- Other information as required by HIPAA privacy rules.

The privacy notice will inform participants that the Company will have access to PHI in connection with its Plan administrative functions. The privacy notice will also provide a description of the Plan's complaint procedures, the name and telephone number of the contact person for further information, and the date of the notice.

The notice of privacy practices shall be placed on the Plan's or the Company's website(onboarding team? And/or www.visionbrokerage.com . The notice also will be individually delivered:

- At the time of an individual's enrollment in the Plan
- To a person requesting the notice
- To participants within 60 days after a material change to the notice

The Plan will also provide notice of availability of the privacy notice (or copy of the privacy notice) at least once every three years in compliance with the HIPAA privacy regulations.

V. Complaints

Sanju Verma, AVP and Lead International HR, 3226 Scott Blvd, Santa Clara CA 95054, 408-327-1254 will be the Plan's contact person for receiving complaints.

The Privacy Official is responsible for creating a process for individuals to lodge complaints about the Plan's privacy procedures and for creating a system for handling such complaints. A copy of the complaint procedure shall be provided to any participant upon request.

VI. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of HIPAA or this HIPAA Privacy Policy will be imposed in accordance with the Company's normal disciplinary policies, up to and including termination.

VII. Mitigation of Inadvertent Disclosures of PHI

The Plan shall mitigate, to the extent possible, any harmful effects that become known to it from a use or disclosure of an individual's PHI in violation of HIPAA or the policies and procedures set forth in this Privacy Policy. As a result, if an employee or business associate becomes aware of an unauthorized use or disclosure of PHI, either by an employee or business associate, the employee or business associate must immediately contact the Privacy Official so that appropriate steps to mitigate harm to the participant can be taken.

VIII. 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 under the Plan

IX. Plan Document

The Plan document shall include provisions to describe the permitted and required use and disclosures of PHI by the Company for plan administrative or other permitted purposes. Specifically, the Plan document shall require the Company to:

- Not use or further disclose PHI other than as permitted by the Plan documents or as required by law;
- Ensure that any agents or subcontractors to whom it provides PHI received from the Plan agree to the same restrictions and conditions that apply to the Company;
- Not use or disclose PHI for employment-related actions;
- Report to the Privacy Official any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;
- Make PHI available to Plan participants, consider any requests for amendments and, upon request, provide them with an accounting of PHI disclosures in accordance with the HIPAA privacy rules;
- Make the Company's internal practices and records relating to the use and disclosure of PHI received from the Plan available to the Department of Health and Human Services (HHS) upon request; and
- If feasible, return or destroy all PHI received from the Plan that the Company still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosure to those purposes that make the return or destruction of the information infeasible.

The Plan document must also require the Company to (1) certify to the Privacy Official that the Plan documents have been amended to include the above restrictions and that the Company agrees to those restrictions, and (2) provide adequate firewalls in compliance with the HIPAA privacy rules.

X. Documentation

The Plan's privacy policies and procedures shall be documented and maintained for at least six years from the later of the date the policies were created or the date the policies were last in effect. Policies and procedures must be changed as 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.

The Plan shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights.

The documentation of any policies and procedures, actions, and designations may be maintained in either written or electronic form. The Plan will maintain such documentation for at least six years.

C. Policies on Use and Disclosure of PHI

I. Use and Disclosure Defined

The Plan will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- *Use.* The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the Benefits, Human Resources or Personnel departments of the Company, or by a Business Associate (defined below) of the Plan.
- *Disclosure*. For information that is PHI, disclosure means any release, transfer, provisions of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within the Benefits, Human Resources or Personnel departments of the Company, or not to a Business Associate (defined below) of the Plan.

II. Workforce Must Comply With Plan's Policy and Procedures

All members of the Company's workforce (described at the beginning of this Policy and referred to herein as "employees") who have access to Plan PHI must comply with this Policy and with the Plan's Privacy Use-and-Disclosure Procedures, which are set forth in a separate document.

III. Permitted Use-and-Disclosures for Plan Administration Purposes

The Plan may disclose to the Company for its use the following: (1) de-identified health information relating to plan participants; (2) Plan enrollment information; (3) summary health information for the purposes of obtaining premium bids for providing health insurance coverage under the Plan or for modifying, amending, or terminating the Plan; or (4) PHI pursuant to an authorization from the individual whose PHI is disclosed.

The Plan may disclose PHI to the following employees who have access to use and disclose PHI to perform functions on behalf of the Plan or to perform plan administrative functions ("employees with access"): Murali Mehrwade, SR. Manager, International HR

Employees with access may disclose PHI to other employees with access for Plan administrative functions (but the PHI disclosed must be limited to the minimum amount necessary to perform the Plan administrative function). Employees with access may not disclose PHI to employees (other than employees with access) unless an authorization

is in place or the disclosure otherwise is in compliance with this Privacy Policy and the Plan's Privacy Use and Disclosure Procedures. Employees with access must take all appropriate steps to ensure that the PHI is not disclosed, available, or used for employment purposes. For purposes of this Policy, "Plan administrative functions" include the payment and health care operation activities described in section C.IV of this Privacy Policy.

IV. Permitted Uses and Disclosures: Payment and Health Care Operations

PHI may be disclosed for the Plan's own payment purposes, and PHI may be disclosed to another covered entity for the payment purposes of that covered entity. For this purpose, payment includes activities undertaken to obtain Plan contributions or to determine or fulfill the Plan's responsibility for provision of benefits under the Plan, or to obtain or provide reimbursement for health care. Payment also includes:

- Eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims
- Risk-adjusting based on enrollee status and demographic characteristics
- Billing, claims management, collection activities, obtaining payment under a contract for re-insurance (including stop-loss insurance and excess loss insurance) and related health care data processing
- Any other payment activity permitted by the HIPAA privacy regulations.

PHI may be disclosed for purposes of the Plan's own health care operations. PHI may be disclosed to another covered entity for purposes of the other covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the participant and the PHI requested pertains to that relationship. For this purpose, health care operations means any of the following activities:

- Conducting quality assessment and improvements activities
- Reviewing health plan performance
- Underwriting and premium rating
- Conducting or arranging for medical review, legal services and auditing functions
- Business planning and development
- Business management and general administrative activities
- Other health care operations permitted by the HIPAA privacy regulations

V. No Disclosure of PHI for Non-Health Plan Purposes

PHI may not be used or disclosed for the payment or operations of the Company's "non-health" benefits (e.g., disability, workers' compensation, life insurance, etc.), unless the participant had provided an authorization for such use or disclosure (as discussed in "Disclosures Pursuant to an Authorization") or such use or disclosure is required or allowed by applicable state law and particular requirements under HIPAA are met.

VI. Mandatory Disclosures of PHI

A participant's PHI must be disclosed, in accordance with Plan's Privacy Use and Disclosure Procedures, in the following situations:

- The disclosure is to the individual who is the subject of the information (see the policy for "Access to Protected Information and Request for Amendment" that follows)
- The disclosure is required by law
- The disclosure is made to HHS for purposes of enforcing HIPAA.

VII. Other Permitted Disclosures of PHI

PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. The Plan's Privacy Use and Disclosure Procedures describe specific requirements that must be met before these types of disclosures may be made. The requirements include prior approval of the Plan's Privacy Official. Permitted disclosures are:

- About victims of abuse, neglect or domestic violence
- For treatment purposes
- For judicial and administrative proceedings
- For law enforcement purposes
- For public health activities
- About decedents
- For cadaveric organ-, eye- or tissue- donation purposes
- For certain limited research purposes
- To avert a serious threat to health or safety
- For specialized government functions
- That relate to workers' compensation programs.

VIII. Disclosures of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the participant. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

IX. Complying With the "Minimum-Necessary" Standard

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use of disclosure.

The "minimum-necessary" standard does not apply to any of the following:

- Uses or disclosures made to the individual
- Uses or disclosures made pursuant to a valid authorization
- Disclosures made to HHS
- Uses or disclosures required by law
- Uses or disclosures required to comply with HIPAA.

Minimum necessary when disclosing PHI
The Plan, when disclosing PHI subject to the minimum necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI that is necessary for the requestor is disclosed. More details on the requirements are found in the Plan's Privacy Use and Disclosure Procedures. All disclosures not discussed in the Plan's Privacy Use and Disclosure Procedures must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum necessary when requesting PHI
The Plan, when requesting PHI subject to the minimum-necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI necessary for the Plan is requested. More details on the requirements are found in the Plan's Privacy Use and Disclosure Procedures. All requests not discussed in the Plan's Privacy Use and Disclosure Procedures must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

X. Disclosure of PHI to Business Associates

Employees may disclose PHI to the Plan's business associates and allow the Plan's business associates to create or receive PHI on its behalf. However, prior to doing so, the Plan must first obtain assurances from the business associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must contact the Privacy Official and verify that a business associate contract is in place. For this purpose, a business associate is an entity that:

- Performs or assists in performing a Plan function or activity involving the use and disclosure of PHI (including claims processing or administration, data analysis, underwriting, etc.)
- Provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

XI. Disclosures of De-Identified Information

The Plan may freely use and disclose information that has been "de-identified" in accordance with the HIPAA privacy regulations. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.

XII. Breach Notification Requirements

The Plan will comply with the requirements of the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") and its implementing regulations to provide notification to affected individuals, HHS, and the media (when required) if the Plan or one of its business associates discovers a breach of unsecured PHI.

D. Policies on Individual Rights

I. Access to PHI and Request for Amendment

HIPAA gives participants the right to access and obtain copies of their PHI that the Plan (or its business associates) maintains in designated record sets. HIPAA also provides that participants may request to have their PHI amended, including the maintenance of any electronic records, as restricted under the HITECH Act. The Plan will provide access to PHI and it will consider requests for amendment that are submitted in writing by participants. For this purpose a designated record set is a group of records maintained by or for the Plan that includes:

- The enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan
- Other PHI used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

II. Accounting

An individual 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, other than disclosures:

- To carry out treatment, payment or health care operations
- To individuals about their own PHI
- Incident to an otherwise permitted use or disclosure
- Pursuant to an authorization
- To persons involved in the individual's care or payment for the individual's care or for certain other notification purposes
- To correctional institutions or law enforcement when the disclosure was permitted without authorization
- As part of a limited data set
- For specific national security or law enforcement purposes
- Disclosures that occurred prior to the compliance date.

The Plan shall respond to an accounting request within 60 days. If the 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. 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 that reasonably informs the individual of the basis for the disclosure (or a copy of the written request for disclosure, if any). If a brief purpose statement is included in the accounting, it must be sufficient to reasonably inform the individual of the basis of the disclosure.

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 accounting.

III. Request for Alternative Communication Means or Locations

Participants may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, participants may ask to be called only at work rather than at home. The Plan may, but is not required to, honor such request. The decision to honor such a request shall be made by the Privacy Official. However, the Plan shall accommodate such a request if the participant clearly states that the disclosure of all or part of the information could endanger the participant. The Privacy Official has responsibility for administering requests for confidential communications.

IV. Request for Restrictions on Use and Disclosure of PHI

A participant may request restrictions on the use and disclosure of the participant's PHI. The Plan may, but is not required to, honor such request. The decision to honor such a request shall be made by the Privacy Official.