HIPAA PRIVACY POLICIES AND PROCEDURES

Introduction

The Procter & Gamble Company and its subsidiaries (collectively, "Company") sponsor certain self-insured group health plans in the United States (collectively, the "Plan"). The Plan amends and restates these HIPAA Privacy Policies and Procedures (referred to herein as the "Policy"). This Policy is intended to comply with the written policy requirements of the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, Subparts A and E, as amended from time to time (the "HIPAA Privacy Rule") and the Health Information Technology for Economic and Clinical Health ("HITECH") Act, contained within the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5. 123 Stat. 226), as amended from time to time. The Plan is a "hybrid entity" as that term is defined under 45 C.F.R. §164.103 and hereby designates, in accordance with 45 C.F.R. § 164.105(a)(2)(iii)(D), the health care components of the Plan identified in Appendix A to this Policy as the components of the Plan that constitute "group health plans" (as defined under HIPAA). The Policy shall only apply to the designated health care components identified in Appendix A. To the extent the Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall not be binding upon the Company or the Plan.

Members of the Company's workforce may have access to the Protected Health Information ("PHI") of Plan participants (1) on behalf of the Plan or (2) on behalf of the Company, for purposes of Plan administrative functions (hereinafter referred to as "Workforce Members"). Workforce Members must comply with the Policy.

The Company reserves the right to amend or change this Policy at any time (even retroactively) without notice. To the extent that portions of this Policy are intended to reflect HIPAA regulations, they shall be deemed to be amended for changes to those regulations as necessary for the Plan to remain in compliance until such time as they are actually amended for such changes.

The Plan's Privacy Official shall have complete power, authority and discretion to determine all matters with respect to the administration of the Policy and to implement and carry out the provisions herein including, but not limited to, the determination and interpretation of all provisions of the Policy, and modification of the Policy from time to time as necessary to comply with any changes in relevant legal requirements including, but not limited to, the HIPAA Privacy Rule.

This Policy does not, and is not intended to, create any third-party rights (including, but not limited to, rights for any Plan participant, beneficiary, dependent, or Business Associate).

TABLE OF CONTENTS

HIPAA Privacy Policies and Procedures

ARTICLE I
DEFINITIONS

The following definitions apply to the terms used in this Policy. Capitalized terms used but not herein defined shall have the meaning attributed to such terms under the Plan or the HIPAA Privacy Rule, as applicable. The following is a partial list of defined terms set forth in the HIPAA Privacy Rule.

"Agent" means a person under the direct control of the Plan or a Business Associate (as applicable) in the performance of his or her work for or on behalf of the Plan, and who is acting within the scope of the agency (e.g., subcontractor). A Business Associate will be the Agent of the Plan only if the Plan retains the authority to control the actions of the Business Associate or to the extent the Plan has delegated responsibilities under HIPAA to the Business Associate.

"Authorization" means a written authorization, that is limited in scope, by an Individual relating to the Use or Disclosure of PHI that satisfies the requirements of Article III, Section V(B).

"Breach" means the acquisition, access, Use, or Disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule that compromises the security or privacy of the PHI.

"Breach" does not include:

- Any unintentional acquisition, access, or Use of PHI by a Workforce Member or a person acting under the authority of the Plan or its Business Associate, if the acquisition, access, or Use was made in good faith and within the scope of the Workforce Member's authority and does not result in further Use or Disclosure in a manner not permitted under the HIPAA Privacy Rule.

- Any inadvertent Disclosure by a person authorized to access PHI at the Plan or its Business Associate to another person authorized to access PHI at the Plan or its Business Associate, and the PHI received as a result of the Disclosure is not further used or Disclosed in a manner not permitted under the HIPAA Privacy Rule.

- A Disclosure of PHI to an unauthorized person where the Plan or its Business Associate (as applicable) has a good faith belief that such unauthorized person would not reasonably have been able to retain the PHI.

Except in the event that one of the exclusions listed above applies, an acquisition, access, Use, or Disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule is presumed to be a Breach unless the Plan or Business Associate (as applicable) demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification;

- The unauthorized person who used the PHI or to whom the PHI was Disclosed;

- Whether the PHI was actually acquired or viewed;

- The extent to which the risk to the PHI has been mitigated; and

Any other factor relevant under the circumstances.**"Business Associate"** means a person (including an entity) who, on behalf of the Plan, but not as a Workforce Member, (1) creates, receives, maintains or transmits PHI for a function or activity regulated by the HIPAA Privacy Rule, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management and repricing; or (2) provides legal, accounting, actuarial, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the Plan, where the performance of such services involves the Disclosure of PHI from the Plan or from another Business Associate to the person. A Business Associate includes a subcontractor that creates, receives, maintains or transmits PHI on behalf of a Business Associate of the Plan. The Company and Workforce Members are not Business Associates of the Plan.

"Business Associate Agreement" means an agreement between the Plan and a Business Associate (or, in the case of a Business Associate who engages a third-party to perform services, between two Business Associates) that addresses the Use and Disclosure of PHI (including, to the extent applicable, ePHI) with respect to the services provided pursuant to an underlying service agreement between the parties. Requirements of Business Associate Agreements are provided in Article III, Section VI.

"Company" means The Procter & Gamble Company and its subsidiaries, including but not limited to The Procter & Gamble U.S. Business Services Company ("GBS"). GBS includes NA My P&G Services & US Benefits Delivery.

"Covered Entity" means the Plan unless otherwise specified.

"De-Identified Health Information" means 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. Information is de-identified only if:

(a) a person with appropriate knowledge and experience with generally accepted statistical and scientific principals and methods for rendering information not individually identifiable: (i) applies such principles and methods to the information and determines that the risk is very small that such information could be used, alone or in combination with other reasonable available information, by an anticipated recipient to identify an individual who is a subject of the information, and (ii) documents the methods and results of the analysis that justify such determination; or

(b) the Plan does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information, and all of the following identifiers of the Individual, his/her relatives, his/her employers and his/her household members are removed

- Names;
- All geographic subdivisions smaller than a state, including street address, city, county, precinct zip code, and their equivalent geocodes except that the initial three digits of a zip code may be used if, according to the current publicly available data from the Bureau of the Census: (i) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and (ii) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000);
- All elements of dates (except year) for dates directly related to an Individual (including birth date, admission date, discharge date, date of death), and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages or elements may be aggregated into a single category of age 90 or older;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security numbers;
- Medical record numbers;
- Health Plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Device identifiers and serial numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code, except as assigned for purposes of re-identification in accordance with the HIPAA Privacy Rule.

"Designated Record Set" means a group of records maintained by or for the Plan that includes:

- medical records and billing records about Individuals maintained by or for a covered health care provider;
- the enrollment, Payment, claims adjudication and case or medical management records maintained by or for the Plan; or
- other PHI Used, in whole or in part, by or for the Plan to make decisions about an Individual.

"Disclose" or "Disclosure" means the Plan's release, transfer, provision of access to, or divulging in any manner of PHI outside of the Plan.

"Electronic PHI" or **"ePHI"** means any PHI that is transmitted or maintained in electronic media (as defined in 45 C.F.R. Section 160.103). All references to PHI in this document shall include ePHI, when applicable.

"Electronic Health Records" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

"GBS" GBS means The Procter & Gamble U.S. Business Services Company, a wholly-owned subsidiary of The Procter & Gamble Company.

"GBS-My P&G Services" GBS-My P&G Services means the Human Resources Services component of GBS, including NA My P&G Services & US Benefits Delivery.

"Genetic Information" means, with respect to an individual, information regarding: (i) the individual's genetic tests, (ii) the genetic tests of family members of the individual, (iii) the manifestation of a disease or disorder in family members of the individual, and (iv) any request for (or receipt of) genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual. Any reference to Genetic Information concerning an individual or family member of an individual shall include the Genetic Information of: (i) a fetus carried by the individual or family member who is a pregnant woman; and (ii) any embryo legally held by an individual or family member utilizing an assisted reproductive technology.

"Health Care Operations" means any of the activities identified as such in the HIPAA Privacy Rule conducted by the Plan. Without limiting the foregoing, Health Care Operations includes:

- conducting quality assessment and improvement activities, patient safety activities, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with

information about Treatment alternatives, and related functions that do not include Treatment;

- reviewing the competence or qualifications of health care professionals, evaluating practitioner, provider or Health Plan performance, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

- except as prohibited under Article III, Section VII, underwriting, enrollment, premium rating, and other activities relating to the creation or renewal or replacement of a contract of health insurance or health benefits, and ceding, securing or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance);

- conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs;

- business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the Plan, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

- business management and general administrative activities, including but not limited to (i) management activities relating to implementation and compliance with the HIPAA Privacy Rule and this Policy, (ii) provision of customer service, including the provision of data analyses for policy holders or the Plan Sponsor, provided that PHI is not Disclosed to such policy holder or Plan Sponsor, (iii) resolution of internal grievances, (iv) the sale transfer, merger or consolidation of all or a part of the Plan with another plan that is subject to the HIPAA Privacy Rule or that following such activity will become subject to the HIPAA Privacy Rule and due diligence related to such activity, and (v) creating De-Identified Health Information or a Limited Data Set.

Note: Other identifiers also must be removed to the extent possible to allow the Plan to complete Health Care Operations without the other identifiers, and to the extent the Company has actual knowledge that the information could be used alone or in combination with other information to identify an Individual who is the subject of the information.

"HHS" means the United States Department of Health and Human Services.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, the HITECH Act, and their implementing regulations, as amended from time to time.""""

"HIPAA Privacy Rule" means the regulations at 45 C.F.R. Part 160 and Part 164, Subparts A and E, as amended from time to time.

"HIPAA Security Rule" means the regulations at 45 C.F.R. Part 164, Subpart C, as amended from time to time.

"HIPAA Breach Notification Rule" means the regulations at 45 C.F.R. Part 164, Subpart D, as amended from time to time.

"HITECH Act" means the Health Information Technology for Economic and Clinical Health Act of 2009 and implementing regulations, as amended from time to time.

"Individual" means the person who is the subject of PHI. The Company shall treat a personal representative as an Individual in accordance with 45 C.F.R. § 164.502(g).

"Individually Identifiable Health Information" means information in any form (i.e., in written, oral or electronic format), including demographic information collected from an individual, that: (i) relates to (a) the past, present or future physical or mental health or condition of an individual; (b) the provision of health care to an individual; or (c) the past, present or future payment for the provision of health care to an individual; and (ii) (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

"Limited Data Set" means PHI from which the following identifiers have been removed:

- Names;
- Postal address information, other than town or city, state and zip code;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet protocol (IP) address numbers;

- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images.

"Minimum Necessary" means limiting the Use or Disclosure of, or request for, PHI to the minimum necessary amount needed to accomplish the intended purpose of the Use, Disclosure or request (as further described in Article VII "Complying with the Minimum Necessary Standard").

"Payment" means, except as prohibited under Article III, Section VII, activities undertaken by the Plan to obtain Plan premiums and contributions or to determine or fulfill the Plan's responsibility for coverage and provision of benefits under the Plan, or to obtain or provide reimbursement for the provision of health care. Without limiting the foregoing, Payment 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 reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing;
- review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
- utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
- Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement (i) name and address; (ii) date of birth; (iii) Social Security number: (iv) payment history; (v) account number; and (vi) name and address of the Plan.

"Plan" means the self-insured group health plans sponsored by the Company for United States employees (including any and all amendments and supplements thereto).

"Plan Sponsor" means The Procter & Gamble Company and its subsidiaries (the Company). The Plan Sponsor is distinguished from the Plan for purposes of the HIPAA Privacy Rule.

"Plan Administration Functions" means the Payment activities and Health Care Operations that the Company or a Business Associate performs on behalf of the Plan. Plan Administration Functions do not include:

- modifying, amending, or terminating the Plan;
- soliciting bids from prospective issuers;

- enrollment functions performed by the Company on behalf of its employees; and

- any employment-related functions or functions in connection with components of the Plan that are not "group health plans" or any of the Company's benefits plans that are not subject to HIPAA, and the benefits provided under such plans.

"Protected Health Information" or **"PHI"** means Individually Identifiable Health Information, excluding information:

(a) in certain "education records" covered by the Family Educational Rights and Privacy Act, as amended (20 U.S.C. §1232g);

(b) in records excluded by the definition of "education records" as described in 20 U.S.C. § 1232(a)(4)(B)(iv) which pertain to a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice;

(c) in employment records held by the Plan Sponsor in its role as employer. Medical information needed for an employer to carry out its obligations under the Family and Medical Leave Act, Americans with Disabilities Act, and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance, and fitness-for-duty tests of employees, may be part of the employment records maintained by the Plan Sponsor in its role as an employer; or

(d) regarding a person deceased for more than 50 years.

References to PHI in this document shall include ePHI, when applicable.

"Qualified Protective Order" means an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that (i) prohibits the parties from using or disclosing PHI for any purpose other than the litigation or proceeding for which such information was requested; (ii) requires the return or destruction of the PHI (including all copies made) at the end of the litigation or proceeding; and (iii) otherwise satisfies the requirements of the HIPAA Privacy Rule for a "Qualified Protective Order" as of the date of the order.

"Summary Health Information" or **"SHI"** means information that may be PHI, that summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom the Plan Sponsor has provided health benefits under the Plan, which has been de-identified (as defined above), except that addresses may be aggregated to the level of a five digit zip code.

"Secretary of HHS" means the Secretary of the Department of Health and Human Services or his or her designee.

"Summary Health Information" means information, which may be Individually Identifiable Health Information, that summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom the Plan Sponsor has provided health benefits under a group Health Plan. Summary Health Information includes information from which the information listed in the definition of "De-identified Health Information" regarding the Individual or relatives, employers or household members of the Individual has been deleted, except the geographic zip code need only be aggregated to the level of five digits.

"Treatment" means the provision, coordination, or management of health care and related services by one or more health care providers (including the provision of preventive and primary care services at the OSMC and through the Plan's wellness programs); the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

"Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the Use of a technology or methodology specified by the Secretary of HHS in the guidance issued under section 13402(h)(2) of Public Law 111-5.

"Use" means, with respect to PHI, the sharing, employment, application, utilization, examination, or analysis of PHI within the Plan.

"Workforce Member" means employees, volunteers, trainees, and other persons of the Plan Sponsor with access to PHI who perform Plan Administration Functions for or on behalf of the Plan as required pursuant to the Plan documents, whose work performance is under the direct control of the Plan. Where the context requires, Workforce Members may include such persons under the direct control of the Company (it its role as a Plan Sponsor). Workforce Member does not include third-party administrators or other Business Associates. A current list of Workforce members is maintained by the HIPAA Privacy Official.

ARTICLE II
PLAN'S GENERAL RESPONSIBILITIES AS COVERED ENTITY

I. **Privacy Official and Contact Person**. The Company's Global Privacy Officer ("Privacy Officer") is the Plan's Privacy Official. The Privacy 'Official's responsibilities include, but are not limited to the following:

- developing a thorough understanding of the HIPAA Privacy Rule and this Policy;
- approving, implementing and enforcing policies and procedures relating to the privacy of PHI, including but not limited to this Policy, including investigating potential violations of this Policy;
- developing necessary and appropriate training programs and schedules for Workforce Members with respect to this Policy and the HIPAA Privacy Rules so they can carry out their Plan Administration Functions in compliance with HIPAA, and ensuring Workforce Members receive such training;
- reviewing requests for and restricting Uses and Disclosures of PHI;
- administering a system for restricting or permitting access to PHI that complies with this Policy;
- ensuring the Plan complies with HIPAA with respect to Business Associates, including the requirement that the Plan have HIPAA-compliant Business Associate Agreements in place with all Business Associates, and monitoring Business Associates' compliance with relevant provisions of Business Associate Agreements, HIPAA and this Policy;
- establishing and monitoring a system for receiving questions and complaints regarding the Plan's privacy practices;
- administering Individual requests under Article IV;
- designating a person or office as a contact person to provide Individuals further information regarding matters covered in the Notice of Privacy Practices issued by the Plan; and
- working with the security, legal and other appropriate departments to develop methods of investigating complaints or allegations of noncompliance with the Policy, and, in conjunction with human resources, the legal department and other appropriate departments, developing appropriate sanctions or disciplinary actions for noncompliance by Workforce Members and Business Associates.

The Privacy Official may delegate all or a portion of his or her responsibilities hereunder to one or more persons, who will be responsible for implementing various aspects of this Policy, provided that such delegation is in writing and maintained in accordance with the documentation requirements set forth in Article VIII.

The Privacy Official is responsible for implementing the Plan's policies and procedures.

No Use or Disclosure of PHI may be made unless it is approved by the Privacy Official, or his or her delegate. Such approval may be granted pursuant to specific approval and/or generally applicable rules and procedures. In any event, the Privacy Official may not approve a Use or Disclosure that is not consistent with this Policy.

II. **Complaints.** The Privacy Official is the contact person identified in the Notice of Privacy Practices responsible for receiving complaints and providing information about the Plan's privacy practices. Any Individual who wishes to make a complaint concerning the Plan's privacy practices or the Plan's compliance with this Policy and HIPAA may do so by submitting such complaint in writing to the Privacy Official at pgprivacyofficer.im@pg.com. Such complaint should include sufficient facts and information to enable the Privacy Official to determine appropriate resolution of the complaint. The Band III Director, NA Health & Wellness My P&G Services & US Benefits Delivery (or equivalent) shall assist with responses to complaints. If related to South Boston On-Site Medical Plan, the Band III Director Boston Site Medical Leader shall assist with responses to complaints. The Individual making a complaint shall be notified in writing of the resolution thereof. Documentation of all complaints and the disposition thereof, if any, shall be documented and retained in accordance with Article VIII.

III. **Workforce Training**. The Company requires all Workforce Members to complete HIPAA Privacy Training with respect to all applicable policies and procedures relating to PHI, including this Policy, before being granted access to PHI, and supplemental training, reminders and updates thereafter on a regular basis. New Workforce Members shall also be provided with such training within a reasonable period of time after joining the Workforce. If there is a material change to this Policy that impacts the Plan functions performed by a Workforce Member, training must be provided to such Workforce Member within a reasonable time after the change becomes effective. The Privacy Official is charged with ensuring that all Workforce Members receive such training, which may be provided in-person, through internet-based materials, or other appropriate means. This Policy is available to Workforce Members for review or reference when needed.

Non-employees with access to PHI and their employer may submit certification of training and HIPAA compliance provided such certifications meet Company standards.

Training with respect to this Policy (including the type and frequency of training) shall be documented and maintained in accordance with Article VIII. In addition, the training program will include procedures to document the training given to each Workforce Member.

IV. **Sanctions for Violations of this Policy**. Sanctions for Using or Disclosing PHI in violation of HIPAA or this Policy, or any other failure to comply with the terms and provisions of this Policy, may be imposed in accordance with the Company's discipline policy and applicable law, up to and including termination of employment, consistent with the Company's employment policy. In determining the appropriate disciplinary action, the Privacy Official shall consider the facts and circumstances, including but not limited to the violation itself and the extent to which the conduct or action was intentional. Depending on the severity of the action, the Workforce Member could be suspended (with or without pay) with no oral or written warning and may be terminated or otherwise disciplined.

Any sanction or disciplinary action imposed in connection with this Section shall be documented and retained in accordance with Article VIII.

V. **Mitigation of Inadvertent Disclosures of PHI**. The Plan shall mitigate, to the extent possible, any harmful effects that become known to it of a Use or Disclosure of an Individual's PHI in violation of HIPAA or this Policy by a Workforce Member or a Business Associate, or as a result of a Breach of Unsecured PHI. If Workforce Members become aware of a Use or Disclosure of PHI, either by other Workforce Members or Business Associates, that is not in compliance with HIPAA or this Policy, they must immediately contact the Privacy Official, copying securityincident.im@pg.com, so that the appropriate steps to mitigate the harm to the Individual can be taken. Contact information for the current Privacy Official, as well as other contacts mentioned in this Policy, are available by jus pgprivacyofficer.im@pg.com for this information.

VI. **No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy**. The Plan may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against Individuals for exercising their rights with respect to their PHI under this Policy or the HIPAA Privacy Rule, including the filing of a complaint, initiating, testifying, assisting or participating in any investigation conducted by the Secretary of HHS, or opposing any improper practice under HIPAA.

The Plan and/or the Privacy Official shall not require any Individual to waive any right granted to such Individual with respect to his or her PHI under HIPAA as a condition of enrollment in or eligibility for benefits under the Plan.

VII. **Modification to this Policy**.

- **Changes Required for Compliance**. The Plan shall make changes to this Policy as necessary and appropriate to comply with changes in the law, including the HIPAA Privacy Rule, and shall promptly document and implement such revised policy or procedure. In the event such change requires a corresponding change in the Plan's Notice of Privacy Practices, a revised Notice of Privacy Practices shall be made available as contemplated by Article V of this Policy. A change to the policy or procedure may not be implemented prior to the effective date of the revised Notice of Privacy Practices, except as otherwise required by law.

- **Documentation**. Written record of any change or revision made in connection with this Section shall be documented and maintained in accordance with Article VIII of this Policy.

VIII. **Compliance Reports and Reviews**:

- **Provide Records and Compliance Reports**. The Plan must keep records and submit compliance reports, in the time and manner, as the Secretary of HHS may determine to be necessary to enable the Secretary of HHS to ascertain the Plan's compliance with the HIPAA Privacy Rule.

- **Cooperate with Compliance Investigations and Reviews**. The Plan shall cooperate with the Secretary of HSS if the Secretary of HHS undertakes an investigation or compliance review of the policies, procedures or practices of the Plan to determine compliance with the HIPAA Privacy Rule.

- **Permit Access to Information**. The Plan shall permit access by the Secretary of HSS during normal business hours to the Plan's facilities, books, records and accounts and other sources of information, including PHI, that are pertinent to ascertaining compliance with the HIPAA Privacy Rule. If any information required of the Plan under this Section shall be in the exclusive possession of any other agency, institution or person and that agency, institution or person fails or refuses to furnish such information, the Plan must so certify and set forth the efforts it made to obtain the information.

IX. **Disclosures to the Plan Sponsor; Plan Document; Certification**. The Plan may not make a Disclosure to the Plan Sponsor unless the requirements of this Article II, Section IX are satisfied.

Except with respect to Genetic Information, the Plan, or third party administrator, health insurance issuer or HMO with respect to the Plan, may Disclose Summary Health Information to the Plan Sponsor, if the Plan Sponsor requests the Summary Health Information for the purpose of: (i) obtaining premium bids from Health Plans for providing health insurance coverage under the Plan; or (b) modifying, amending, or terminating the Plan.

The Plan, or the third-party administrator, health insurance issuer or HMO with respect to the Plan, may Disclose to the Plan Sponsor information on whether an Individual is participating in the Plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the Plan.

The Plan or the third-party administrator may make a Disclosure to the Plan Sponsor for Plan Administration Functions provided that the Plan document includes, and the Plan is administered in accordance with, provisions to:

- Establish the permitted and required Uses and Disclosures of such information by the Plan Sponsor, provided that such permitted and required

Uses and Disclosures may not be inconsistent with the HIPAA Privacy Rule or this Policy; and

- Provide that the Plan will Disclose PHI to the Plan Sponsor only upon receipt of a certification by the Plan Sponsor that the Plan documents have been amended to incorporate the following provisions and that the Plan Sponsor agrees to:

  - not Use or further Disclose PHI other than as permitted by the Plan documents or as required by law;

  - ensure that any Agents (e.g., subcontractors) to whom it provides PHI received from the Plan agree to the same restrictions and conditions that apply to the Plan Sponsor with respect to such information;

  - not Use or Disclose PHI for employment-related actions or in connection with any other employee benefit plan of the Plan Sponsor;

  - report to the Plan any Use or Disclosure of the information that is inconsistent with the permitted Uses or Disclosures under HIPAA and this Policy of which the Plan Sponsor becomes aware; - make PHI accessible to Individuals in accordance with Article IV, Section II of this Policy;

  - allow Individuals to amend their PHI and incorporate any amendments of their PHI in accordance with Article IV, Section III of this Policy;

  - upon request, provide Individuals with an accounting of PHI Disclosures in accordance with Article IV, Section IV of this Policy;

  - make the Plan Sponsor's internal practices and records relating to the Use and Disclosure of PHI received from the Plan available to the Secretary of HHS upon request for purposes of determining compliance with the HIPAA Privacy Rule;

  - if feasible, return or destroy all PHI received from the Plan that the Plan Sponsor 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 Disclosures to those purposes that make the return or destruction of the information infeasible;

  - ensure that adequate separation exists between the Plan and the Plan Sponsor as set forth below;

  - provide for adequate separation between the Plan and the Plan Sponsor by including provisions that:

    - describe those Workforce Members or classes of Workforce Members or other persons under the control of the Plan Sponsor to

be given access to the PHI to be Disclosed, provided that any Workforce Member or person who receives PHI relating to Payment, Health Care Operations or other matters pertaining to the Plan in the ordinary course of business must be included in such description;

- restrict access to and use by such Workforce Members and other persons described above to the Plan Administration Functions that the Plan Sponsor performs for the Plan; and

- provide an effective mechanism for resolving any issues of noncompliance by persons described above with the Plan document provisions required by this Article II, Section IX.

The Plan Sponsor hereby certifies to the Plan that the Plan documents have been amended to include the above restrictions and the Plan Sponsor is in compliance with the HIPAA Privacy Rule. Further, the Plan Sponsor shall provide adequate firewalls in compliance with the HIPAA Privacy Rule.

X. **Miscellaneous Restrictions**.

The Plan may not:

1. Permit a health insurance issuer, third-party administrator or HMO, with respect to the Plan, to Disclose PHI to the Plan Sponsor except as permitted by this Policy;

2. Disclose and may not permit a third-party administrator, health insurance issuer or HMO to Disclose PHI to the Plan Sponsor as otherwise permitted by this Policy unless a statement that the health insurance issuer or HMO may Disclose PHI to the Plan Sponsor is included in the Notice of Privacy Practices; and

3. Disclose PHI to the Plan Sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the Plan Sponsor.

ARTICLE III
USE AND DISCLOSURE OF PHI

The Plan may Use and Disclose PHI only as permitted or required under the terms of this Policy or the HIPAA Privacy Rule. All Workforce Members must comply with this Policy and may not Use or Disclose PHI for any purpose other than in accordance with HIPAA Privacy Rule or the terms of this Policy.

I. **Permitted Uses and Disclosures**.

A. **Procedure**. The Privacy Official (or his or her designee(s)) shall require all Workforce Members who have access to or handle PHI to review this Policy. Uses and Disclosures of PHI for the purposes described under Section B below may generally be made without consulting the Privacy Official or the Band III Director, NA Health & Wellness My P&G Services & US Benefits Delivery / Band III Director Boston Site Medical Leader (or equivalent) (provided the Plan complies with the Individual Rights HIPAA Privacy Compliance Policy concerning an Individual's right to request restrictions on the Plan's handling of certain PHI or to request confidential communications of certain PHI). Workforce Members who are uncertain as to whether a Use or Disclosure may be made under Section B must consult the Privacy Official or Band III Director, NA Health & Wellness My P&G Services & US Benefits Delivery / Band III Director Boston Site Medical Leader (or equivalent) before making the Use or Disclosure. Any Use or Disclosure must satisfy the Minimum Necessary Standard (as described in Article VII of this Policy) and be documented in accordance with Article VIII of this Policy, "Documentation, Maintenance and Destruction of PHI."

B. **Permitted Uses or Disclosures**. The Plan is permitted, but not required, to Use and Disclose PHI as follows:

1. **Plan Administration Functions**. The Plan may Disclose the following information to the Plan Sponsor for the 'Plan Sponsor's Uses, including Plan Administration Functions, provided the requirements set forth in Article II, Section IX are met:

- De-Identified Health Information relating to Plan participants for any purpose;
- Information as to whether an Individual has enrolled or dis-enrolled in the Plan or any coverage option thereunder;
- Plan premiums applicable to or paid by an Individual;
- Plan enrollment/disenrollment information for any purpose;
- 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

- PHI pursuant to a valid Authorization (*see Section V of this Article*) from the Individual whose PHI is Disclosed and limited to the purpose described in such Authorization.

2. **Payment**. The Plan may Use or Disclose the Minimum Necessary PHI to carry out Payment, including the Plan's own payment purposes (e.g., premiums); determining and fulfilling responsibilities for coverage and provision of benefits; or furnishing or obtaining reimbursement for health care (e.g., payment to another covered entity (including a health care provider)).

3. **Health Care Operations**. The Plan may Use or Disclose the Minimum Necessary PHI to carry out the Plan's own Health Care Operations or to another covered entity for purposes of the other covered entity's Health Care Operations, if the other covered entity has (or had) a relationship with the Plan participant and the PHI requested pertains to that relationship.

4. **Treatment**. The Plan may Use or Disclose the Minimum Necessary PHI to carry out Treatment activities of a health care provider.

5. **Disclosure of PHI to Business Associates of the Plan**. The Plan may Disclose PHI to a Business Associate and allow the Business Associate to create or receive PHI on behalf of the Plan, provided the requirements with respect to Business Associates set forth below in Section VI of this Article III are met.

6. **To the Individual**. The Plan may disclose PHI to the Individual to whom the PHI relates. Upon receiving a request from an Individual for Disclosure of the Individual's own PHI, the Plan must follow the procedures with respect to an Individual's request as set forth in Article IV of this Policy.

7. **For Communications about Treatment Alternatives and Health-related Benefits/Services**. The Plan may Use PHI to contact an Individual and tell them about possible alternative treatments or health-related benefits or services that are included in a plan of benefits of the Plan that may be of interest to that Individual.

8. **Use or Disclosure Pursuant to an Agreement where the Individual had an Opportunity to Agree or Object**. The Plan may Use or Disclose PHI in certain circumstances where the Plan obtained informal permission form the Individual as described in Section III of this Article III.

9. **Use or Disclosure where Individual Agreement or Objection is not Necessary**. In certain circumstances, as detailed in Section IV of this Article III, the Plan may Use or Disclose PHI without the Individual's

Consent, Authorization or an opportunity for the Individual to agree or object, including when the Plan may Use or Disclose PHI as required by law or for purposes related to judicial or administrative proceedings.

10. **Fundraising Activities**. The Plan may Use or Disclose PHI as permitted by and in compliance with the provisions of the HIPAA Privacy Rule relating to certain fundraising and marketing activities.

11. **To Create De-Identified Health Information**. The Plan may Disclose PHI to create information that is De-identified Health Information, provided that any Disclosure for this purpose may only be to a Business Associate. De-Identified Health Information is not PHI. The Plan may freely Use and Disclose De-Identified Health Information except that:

    (i) disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of PHI that is subject to the disclosures rules of the HIPAA Privacy Rule and this Policy; and

    (ii) if De-identified Health Information is re-identified, the Plan may only use such re-identified information as required or permitted by the terms of this Policy or the HIPAA Privacy Rule.

12. Pursuant to a Valid Authorization. The Plan may Use or Disclose PHI pursuant to and in compliance with a valid Authorization under 45 C.F.R. § 164.508 (as described further in this Article III, Section V, below)

C. **Uses and Disclosures Pursuant to Consent.** As described above, the Plan may Use or Disclose PHI for to carry out Treatment, Payment or Health Care Operations without obtaining the Individual's Consent or Authorization. If the Plan determines that it is appropriate or desirable to seek Consent, the following provisions will apply.

1. **Required Elements of Consent**. For purposes of this Policy, a Consent is a document written in plain language that:

    (i) Informs the Individual that the PHI may be Used and Disclosed to carry out Treatment, Payment, or Health Care Operations;

    (ii) Refers the Individual to the Notice of Privacy Practices contemplated in Article V of this Policy and states that the Individual has the right to review the Notice of Privacy Practices prior to signing the consent;

    (iii) States that the privacy practices described in the Notice of Privacy Practices may change and describes how the Individual may obtain a revised Notice of Privacy Practices;

(iv) States that the Individual has the right to request that the Plan restrict how PHI is Used or Disclosed to carry out Treatment, Payment, or Health Care Operations, that the Plan is not required to agree to the requested restrictions; and that if the Plan agrees to a requested restriction, the restriction is binding on the Plan.

(v) States that the Individual has the right to revoke the Consent in writing, except to the extent that the Plan has taken action in reliance thereon; and

(vi) Is signed by the Individual and dated.

2. **Refusal of Consent**. The PHI of an Individual who is asked by the Plan to provide Consent but refuses to provide such Consent may not be Used or Disclosed, even if the Plan was not required by this Article III or the HIPAA Privacy Rule to request such Consent.

3. **Revocation of Consent**. An Individual may revoke a Consent at any time, except to the extent the Plan has taken action in reliance on the Consent.

4. **Enrollment Condition on Consent**. The Plan may choose to condition enrollment in the Plan on the Individual's signed Consent provided such consent meets the requirements set forth in Section I(C)(1) of this Article III and is sought in conjunction with enrollment in the Plan.

5. **Combination of Consent with Other Types of Permission**. A Consent may be combined with other types of written legal permission from the Individual (e.g., assignment of benefits), provided (a) the Consent is visually and organizationally separate from such other written legal permissions; and (b) the Consent is signed or initialed by the Individual and dated. In any event, a Consent may not be combined with the Notice of Privacy Practices addressed in Article V of this Policy.

6. **Documentation**. Every Consent received by the Plan shall be retained in accordance with Article VIII of this Policy. Every failed attempt to obtain a Consent and the reason for the failure also must be documented.

II. **Required Uses and Disclosures**. The Plan is required to Disclose PHI as follows:

- **Individual Requests**. Upon the Individual's request, in connection with the Individual's right to: (i) access his or her PHI as set forth in Article IV, Section II of this Policy or (ii) receive an accounting of disclosures as set forth in Article IV, Section IV of this Policy.

- **HHS Investigations**. Upon request by the Secretary of HHS to investigate or determine the Plan's compliance with the HIPAA Privacy Rule.

III. **Uses and Disclosures Requiring Opportunity to Agree or Object**. The Plan may, without obtaining **Consent or** Authorization, Use or Disclose PHI, provided that the Individual is informed in advance of the Use or Disclosure and has the opportunity to agree or object. The Plan may orally inform the Individual of and obtain the Individual's oral agreement or objection for the following purposes or situations:

- **Disclosure to Person Involved with Health Care.** In accordance with Sections III(A) and III(B) of this Article III, Disclosure may be made to an Individual's relative, close personal friend, or another person designated by the Individual to the extent that the information disclosed is directly relevant to such person's involvement with the Individual's health care or payment related to the Individual's health care.

- **Use or Disclosure for Notification Purposes**. In accordance with Sections III(A), III(B) and III(C) of this Article III, Use or Disclosure may be made to notify or assist in the notification of (including identifying or locating) a family member, a personal representative of the Individual, or another person responsible for the care of the Individual or the Individual's location, general condition or death.

A. **Opportunity to Agree or Object When Individual is Available**. If the Individual is available prior to a Use or Disclosure described above and has the capacity to make health care decisions, the Plan may Use or Disclosure PHI only if the Plan: (a) obtains the Individual's agreement; (b) provides the Individual with an opportunity to object and the Individual does not express an objection; or (c) reasonably infers from the circumstances, based on the Plan's exercise of professional judgment, that the Individual does not object to the Use and Disclosure. The requirements in this Section may be satisfied orally or in writing.

B. **Use and Disclosure When Individual is Not Available**. If the Individual is not present, or the opportunity to agree or object to the Use or Disclosure cannot practicably be provided because the Individual is incapacitated or due to an emergency situation, the Plan may, based on its exercise of professional judgment, Disclose PHI that is directly relevant to the person's involvement with the Individual's health care or payment for such care, if doing so is, in the Plan's judgment, in the Individual's best interest. The Plan may use professional judgment and its experience with common practice to make reasonable inferences on the Individual's best interest in allowing a person to act on behalf of the Individual to pick up filled prescriptions, medical supplies, X-rays or other similar forms of PHI. In addition, if the Individual is deceased, the Plan may, based on its exercise of professional judgment, Disclose PHI that is relevant to the person's involvement with the Individual's health care or payment for such care prior to death, unless doing so is inconsistent with any prior expressed preference of the Individual that is known to the Plan.

C. **Disaster Relief**. The Plan may Use or Disclose PHI to a public or private entity authorized by law or its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the Uses or Disclosures permitted for notification

purposes as described in this Section. The requirements in Sections III (A) and III (B) above apply to such Uses and Disclosures to the extent that the Plan, in its exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

IV. **Uses and Disclosures That Do Not Require Consent, Authorization or an Opportunity to Agree or Object**. The Plan may Disclose the Minimum Necessary PHI when required to do so by federal, state or local law or for one of the purposes described below, in accordance with the rules described in this Policy and with the HIPAA Privacy Rule.

A. **Procedure**. All Uses and Disclosures provided below must be approved by the Privacy Official before they are made. The determination of whether a Disclosure is permitted by these procedures shall be made by the Privacy Official using this Policy, and these procedures and after conferring with the Company's legal or other consultants. An Authorization from the Individual is not required for these Disclosures. Once a Disclosure is approved, the Privacy Official or designated Workforce Member must take the following steps:

1. **Verify**. Verify the identity and authority of the person or entity seeking the PHI, using conventional means to identify that person (e.g., driver's license, state ID), affiliation (e.g., government badge or ID card) or entity (e.g., letter on government agency letterhead).

2. **Minimum Necessary**. Determine the Minimum Necessary Disclosure under the circumstances using the policies and procedures described in Article VII of this Policy.

3. **Disclosure Log**. Log the Disclosure pursuant to, and to the extent required by Article VIII of this Policy, "Documentation, Maintenance and Destruction of PHI."

B. **Use or Disclosure**. Following are the certain purposes and situations in which the Plan may be permitted to Use and Disclose PHI without the Individual's Consent, Authorization or an opportunity for the Individual to agree or object:

1. **Required by Law**. The Plan may Use or Disclose PHI as permitted to the extent required by law, provided that such Use or Disclosure is limited to the relevant requirements of such law.

2. **Reporting Abuse, Neglect, or Domestic Violence**. The Plan may Disclose PHI about an Individual whom the Plan reasonably believes is a victim of abuse (including child abuse), neglect or domestic violence to a government authority authorized by law to receive such reports , provided that:

- The Disclosure is required by law and the Disclosure complies with and is limited to the relevant requirements of such law;

- The Individual agrees with the Disclosure; or

- The Disclosure is expressly authorized by statute or regulation and the Plan, in the exercise of professional judgement, deems the Disclosure necessary to prevent harm to the Individual (or other victim) or the Individual is incapacitated and unable to agree and information will not be used against the Individual and is necessary for an imminent enforcement activity. In this case, the Individual must be promptly informed of the Disclosure unless this would place the Individual at risk or if informing would involve a personal representative who is believed to be responsible for the abuse, neglect or violence.

3. **Judicial or Administrative Proceedings**. The Plan may Disclose PHI for purposes related to judicial or administrative proceedings, such as in response to:

- An order of a court or administrative tribunal (Disclosure must be limited to PHI expressly authorized by the order); or

- A subpoena, discovery request or other lawful process, not accompanied by a court order or administrative tribunal, provided (i), (ii) and (iii) below are met:

(i) the party seeking the Disclosure provides the Plan a written statement and accompanying documentation demonstrating that:

(a) the requesting party made a good faith attempt to provide written notice to the Individual (or, if the Individual's location is unknown, that the requesting party mailed a notice to the Individual's last known address);

(b) such notice included sufficient information about the litigation or proceeding to allow the Individual to object to the court or administrative tribunal; and

(c) the time for the Individual to object has elapsed and no objections were filed or all objections filed have been resolved by the court or administrative tribunal and the Disclosure sought is consistent with such resolution;

(ii) the party seeking the Disclosure provides the Plan a written statement and accompanying documentation demonstrating that:

(a) the parties to the applicable dispute agreed to a Qualified Protective Order and presented it to the court or administrative tribunal; or

(b) the party seeking the Disclosure requested a Qualified Protective Order from the court or administrative tribunal; and

(iii) the Plan makes reasonable efforts to provide notice that would satisfy the above or seek a Qualified Protective Order.

4. **Law Enforcement Purposes**. The Plan may Disclose PHI to a law enforcement official for law enforcement purposes, if the Disclosure is:

- **Pursuant to Process**. (i) Required by law, subject to Article III, Section IV(B)(1) of this Policy, or (ii) (a) is in compliance with and pursuant to a court order, a court-ordered warrant, a subpoena or a summons issued by a judicial officer, (b) a grand jury subpoena, or (c) an administrative request, a civil or authorized investigative demand, or similar process otherwise required by law, but only if (1) the information sought is relevant and material to a legitimate law enforcement inquiry, (2) the request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought and to the amounts reasonably necessary, and (3) it is not possible to Use De-Identified Health Information;

- **Identification and Location Purposes**. In response to a law enforcement official's request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person, as long as the information is limited to the following information: (i) name and address, (ii) date and place of birth, (iii) Social Security number, (iv) ABO blood type and rh factor, (v) type of injury, (vi) date and time of treatment, (vii) date and time of death (if applicable), and (viii) a description of distinguishing physical characteristics (e.g., height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars and tattoos). The Plan may not disclose PHI related to the Individual's DNA, DNA analysis, dental records, or typing, samples, or analysis of bodily fluids or tissue;

- **About Crime Victims**. Subject to Article III, Section IV(B)(2) of this Policy, in response to a law enforcement official's request for information about a person who is or is suspected to be a victim of a crime, as long as (i) the Individual agrees to Disclosure; or (ii) if the Individual is unable to agree (e.g., incapacitated or due to an emergency situation) and there is an urgent need for the information to determine whether a crime has occurred, provided that (a) the law enforcement official represents that the information

is needed to determine whether a violation of a law by a person other than the Individual has occurred, and the information will not to be used against the victim, (b) the law enforcement official represents that immediate law enforcement activity that depends on the Disclosure would be materially or adversely affected by waiting until the Individual is able to agree, and (c) the Disclosure is, based on the Plan's exercise of professional judgment, in the victim's best interests;

- **Decedents**. For the purpose of alerting a law enforcement official of the Individual's death, as long as the Workforce Member has a suspicion that the Individual's death may have resulted from criminal conduct;

- **Crime on Premises**. Where the Plan believes in good faith the PHI to be evidence of criminal conduct that occurred on the premises of the Plan; or

- **Reporting Crime in Emergency Situation**. Subject to Article III, Section IV(B)(2) of this Policy, if the Plan is a health care provider that is providing emergency health care off the Plan's premises, the Plan may make a Disclosure of PHI to a law enforcement official if such Disclosure appears necessary to alert law enforcement to (i) the commission and nature of the crime; (ii) the location of such crime or the victim(s) of such crime; and (iii) the identity, description and location of the perpetrator of the crime.

5. **For Cadaveric Organ, Eye or Tissue Donation Purposes**. The Plan PHI to an organ procurement organization or other entity engaged in the procurement, banking, or transplantation of organs, eyes or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

6. **For Research Purposes**. The Plan may Use or Disclose PHI for certain limited research purposes provided that (a) a waiver of the Authorization has been approved by an appropriate privacy board (e.g., institutional review board), (b) the waiver is properly documented, in accordance with HIPAA requirements, and (c) the Plan obtains from the researchers certain representations and documentation required by HIPAA.

7. **For Specialized Government Functions**. The Plan may Disclose PHI for the following specialized government functions:

   - To appropriate military command authorities (including foreign military authorities), as long as (a) the purpose has been deemed necessary by such authorities to assure the proper execution of a military mission; (b) the PHI belongs

to Armed Forces personnel (or, in the case of foreign military authorities, foreign military personnel); and (c) such authorities have published in the Federal Register a notice that includes the military command authorities and the purpose for which the PHI may be used and Disclosed; and

- To authorized federal officials for the purpose of conducting national security activities or protecting the President and certain other persons.

- To authorized federal officials for the provision of protective services to the President or other governmental officials.

- To a correctional institution or a law enforcement official having lawful custody of an inmate to whom the PHI pertains.

8. **For Workers' Compensation Programs**. The Plan may Disclose PHI to the extent necessary to comply with laws relating to workers' compensation or other similar programs established by law that provide benefits for work-related injuries or illness without regard to fault.

9. **Public Health Activities**. The Plan may Disclose PHI for public health activities and purposes as follows*:*

- Disclosure to a public health authority authorized by law to collect or receive such information for the purpose of preventing or controlling disease injury or disability;

- Disclosure to person subject to the jurisdiction of the Food and Drug Administration (FDA) to (i) report adverse events (or similar reports with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations; (ii) to track FDA-regulated products; (iii) to enable product recalls, repairs, replacement or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn or are the subject of the lookback); or (iv) to conduct post marketing-surveillance to comply with requirements or at the direction of the FDA; and

- Disclosure to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading disease or condition, if the Plan is authorized by law to notify such person as necessary in the conduct a public health intervention or investigation.

- Disclosure to an employer about a member of the employer's Workforce provided that the following elements are satisfied:

    - The Disclosure is made by a health care provider who is a Covered Entity and is a member of the employer's Workforce or who provides health care to the Individual at the employer's request in order to conduct an investigation relating to medical surveillance of the workplace or to evaluate whether the Individual has a work-related illness or injury;

    - The Disclosed PHI consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

    - The employer needs such findings to comply with its obligations under the Occupational Health Safety Act or the Federal Mine Safety and Health Act, or under similar state law, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and

    - The health care provider who is a Covered Entity provides written notice to the Individual that PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer (1) by giving a copy of the notice to the Individual at the time the health care is provided; or (2) if the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

- Disclosure to a school about an Individual who is a student or prospective student of the school if:

    - The PHI that is Disclosed is limited to proof of immunization;

    - The school is required by law to have such proof of immunization prior to admitting the Individual; and

- The Plan obtains and documents the agreement to the Disclosures from either a parent or legal guardian of the Individual, if the Individual is an unemancipated minor, or if the Individual is an adult or emancipated minor.

10. **Health Oversight Activities**. The Plan may Disclose PHI to a health oversight agency for oversight activities authorized by law necessary for appropriate oversight of the following: (i) the health care system; (ii) government benefit programs for which health information is relevant to beneficiary eligibility; (iii) entities subject to governmental regulatory programs for which health information is necessary for determining compliance with program standards; or (iv) entities subject to civil rights law for which health information is necessary for determining compliance. Disclosures may not be made, however, for oversight activities that are an investigation (or other activity) of the Individual and the investigation (or activity) does not arise out of and is not directly related to the receipt of healthcare, a claim for public benefits related to healthcare, or qualifications for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

11. **Threats to Health or Safety**. Use or Disclosure of PHI is permitted if the Plan, in good faith, believes that the Use or Disclosure is necessary:

    - to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and, if a Disclosure, the Disclosure is made to a person or persons who are reasonably able to prevent or lessen the threat, including the target of the threat.

    - for law enforcement authorities to identify and apprehend an Individual because of a statement by an Individual admitting participation in a violent crime that the Plan reasonably believes may have caused serious physical harm to the victim. Notwithstanding the foregoing, Use or Disclosure may not be made if the information is obtained in the course of treatment, therapy or counseling to affect the propensity to commit the criminal conduct that is the basis of the Disclosure or through a request by the Individual to initiate or be referred for such treatment or therapy or counseling. Such Disclosure is limited to the information described in the "For Identification and Location Purposes" section, above.

    - for law enforcement authorities to apprehend an Individual where it appears from all the circumstances that the Individual has escaped from a correctional institution or from lawful custody.

12. **For Decedents**. Disclosure of PHI may be made to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. Disclosure also may be made to funeral directors, consistent with applicable law, as necessary to carry out the funeral director's duties with respect to the decedent. To the

extent necessary for a funeral director to perform his duties, such disclosure may be made prior to, and in reasonable anticipation of, the Individual's death.

13. **Disability**. Disclosure of PHI may be made as authorized by and to the extent necessary to comply with obligations under the Family and Medical Leave Act, Americans with Disabilities Act, and similar laws; to determine disability insurance eligibility; and to review sick leave requests and justifications.

V. **Uses and Disclosures of PHI Requiring Authorization**. Except as described above, the Company may not Use or Disclose PHI without a valid Authorization, as described in this Section V.

A. **Procedure**. Any requested Disclosure that does not fall within one of the categories for which Disclosure is permitted or required under the procedures as described above may be made pursuant to a valid HIPAA authorization. The Plan and Workforce Members shall not make any Use or Disclosure pursuant to an Authorization unless the Verification Procedures (*see* Article IV, Section VI) have been followed and the identity of the Individual has been verified and the requirements outlined below are met.

B. **Elements of a Valid Authorization**.

1. **Core Elements**. A valid Authorization requires the following core elements:

- A description of the information to be Used or Disclosed that identifies the information in a specific and meaningful fashion.
- The name or other specific identification of the person(s), or class of persons, authorized to make the requested Use or Disclosure.
- The name or other specific identification of the person to whom the Use or Disclosure may be made.
- A description of each purpose of the requested Use or Disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an Individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.
- The Authorization's expiration date, specific time period (e.g., one year from the date of signature), or an expiration event directly relevant to the Individual or the purpose of the

Use or Disclosure (e.g., for the duration of the Individual's coverage).

- Signature of the Individual and date. If the authorization is signed by a personal representative of the Individual, a description of such representative's authority to act for the Individual must also be provided.

2. **Required Statements**. In addition to the core elements, the Authorization must contain statements adequate to place the Individual on notice of all of the following:

   - The Individual's right to revoke the Authorization in writing, and either the exceptions to the right to revoke and a description of how the Individual may revoke the Authorization or a copy of the Plan's Notice of Privacy Practices containing the revocation procedure.

   - The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the Authorization.

   - The potential for the information Disclosed pursuant to the Authorization to be subject to redisclosure by the recipient and no longer be protected by this Policy or the HIPAA Privacy Rule because the Plan no longer has control of such information and the person(s) who received the authorized Disclosure may not be a Covered Entity subject to the HIPAA Privacy Rule.

3. **Other Requirements**. In addition to the Core Elements and Required Statements, the following requirements must be met:

   - The authorization must be written in plain language.

   - Any Use or Disclosures made pursuant to a valid Authorization must be consistent with the terms and conditions of the Authorization.

   - If the Plan seeks an Authorization from an Individual for a Use or Disclosure of PHI, the Plan must provide the Individual with a copy of the signed Authorization.

   - Disclosures must be documented in accordance with Article VIII, "Documentation, Maintenance and Destruction of PHI."

4. **Defective Authorization**. An Authorization is not valid if any of the following defects exist:

- The Authorization's expiration date occurred or the Plan knows the expiration event occurred;
- The Authorization is incomplete as to or lacks a required item described above;
- The Plan knows that the Individual revoked the Authorization;
- The Authorization is combined with another document other than as permitted below;
- The Plan knows that material information in the Authorization is false; or
- The Plan conditions Payment, Treatment, or Health Care Operations on the Authorization except as permitted as follows:
    - Plan enrollment and/or eligibility for benefits may be conditioned on the provision of an Authorization required by the Plan prior to enrollment, provided that (i) the Authorization is sought for the Plan's enrollment and/or eligibility determinations relating to the Individual or for its underwriting or risk rating determinations, and (ii) the Authorization is not for a Use or Disclosure of psychotherapy notes, as described below.
    - Provision of health care that is solely for the purpose of creating PHI for Disclosure to a third party may be conditioned on the provision of an Authorization for the Disclosure of such PHI to such third party.

5. **Combining an Authorization with other Documents.** Generally, an Authorization may not be combined with another document, except as follows:

- An Authorization for a Use or Disclosure of PHI for a research study may be combined with any other type of written permission for the same or another research study, including an Authorization for the creation or maintenance of a research database or repository, or with a consent to participate in such research;
- Authorization for a Use or Disclosure of psychotherapy notes may be combined with another Authorization for a Use or Disclosure of psychotherapy notes;

- An Authorization, other than for a Use or Disclosure of psychotherapy notes, may be combined with another Authorization, provided that an Authorization on which the Plan conditions Payment, Treatment, or Health Care Operations (as described in above in this Article III, Section V (B)(4)) may not be combined with another Authorization.

6. **Revocation of Authorization**. An Individual may revoke an Authorization at any time in writing, provided that an Authorization may not be revoked to the extent that the Plan has relied on the Authorization or, if the Authorization was obtained as a condition for obtaining insurance coverage, the insurer is permitted by law to contest a claim under the policy.

C. **Uses and Disclosures that Require a Valid Authorization**. The Plan may not Use or Disclosure PHI without a valid Authorization for the following Uses or Disclosures:

- **Psychotherapy Notes**. The Plan may not Use or Disclose psychotherapy notes (which are a subset of mental health records and are defined as notes recorded in any medium by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session) without a valid Authorization, unless (a) the Use or Disclosure is to the originator of the notes for treatment purposes; (b) the Use or Disclosure is to defend the Plan in a legal action or proceeding brought by the Individual, (c) the Use or Disclosure is required by HHS, or (d) the Use or Disclosure is permitted because the Disclosure is (i) required by law, (ii) to a health oversight agency for oversight activities related to the originator of the notes, (iii) to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties authorized by law, or (iv) to prevent or lessen a serious or imminent threat to the health or safety of a person or the public.

- **Marketing**. The Plan may not Use or Disclose PHI for marketing purposes without a valid Authorization, unless the communication is (a) a face-to-face communication between the Plan and the Individual, or (b) a promotional gift of nominal value from the Plan to the Individual. Further, the Plan may not receive financial remuneration from a third party with respect to any marketing unless a valid Authorization states that remuneration is involved. Note, however, contacting Individuals to communicate treatment alternatives or other health-related benefits or services that are included in the benefits of Plan that may be of interest to the individual does not constitute marketing.

- **Sale**. The Plan may not sell PHI without a valid Authorization that includes a statement that such Disclosure will result in remuneration to the Plan. For this purpose, "sale" includes any Use or Disclosure where the Plan directly or indirectly receives remuneration, including nonfinancial benefits, from or on behalf of the recipient of the PHI, in exchange for the PHI.

VI. **Disclosures to Business Associates**. The Plan may disclose PHI to a Business Associate and may allow a Business Associate to create or receive PHI on its behalf, provided the Plan obtains written assurances that meet the requirements of this Article III, Section VI, that the Business Associate will appropriately safeguard the information. A Business Associate may not:

- Use or Disclose PHI unless permitted or required by the applicable Business Associate Agreement (as described below) or as required by law;

- Use or Disclose PHI in a manner that would violate the requirements of the HIPAA Privacy Rule if done by the Plan (with certain limited exceptions); or

- Disclose PHI to another Business Associate who is a subcontractor and permit the subcontractor to create, receive, maintain or transmit such information, unless it obtains written assurances from the subcontractor that meet the requirements of this Article III, Section VI, that the subcontractor will appropriately safeguard the information.

A. **Business Associate Agreement Requirements**. The Plan may make a Disclosure to a Business Associate and may allow a Business Associate to create or receive PHI on its behalf, pursuant to a Business Associate Agreement. The Business Associate Agreement governing the services provided or function performed by the Business Associate shall contain provisions that:

1. Establish the permitted and required Uses and Disclosures of PHI by the Business Associate, provided that such permitted and required Uses and Disclosures may not be inconsistent with the obligations of the Plan to comply with any requirements of the HIPAA Privacy Rule or this Policy, except that the Business Associate may be permitted to Use the PHI for its own proper management and administration as contemplated by the HIPAA Privacy Rule; and

2. Provide that the Business Associate will:

(i) Not Use or further Disclose PHI other than as permitted or required by the agreement or as required by law, provided that any Use or Disclosure of PHI be reasonably limited to a Limited Data Set or the Minimum Necessary as required by Article VII of this Policy;

(ii) Use appropriate safeguards and comply, where applicable, with the Security Rule with respect to electronic PHI to prevent Use or Disclosure of the PHI other than as provided for by its agreement;

(iii) Report to the Plan any Use or Disclosure of the PHI not provided for by its agreement of which it becomes aware, including Breaches of Unsecured PHI;

(iv) Ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions and conditions that apply to the Business Associate with respect to such information;

(v) Make available PHI in accordance with Article IV of this Policy;

(vi) Make available PHI for amendment and incorporate any amendments to PHI in accordance with Article IV of this Policy;

(vii) Make available the information required to provide an accounting of Disclosures in accordance with Article IV of this Policy;

(viii) To the extent the Business Associate is to carry out the Plan's obligations under the HIPAA Privacy Rule, comply with the requirements of the HIPAA Privacy Rule that apply to the Plan in the performance of such obligations;

(ix) Make its internal practices, books and records relating to the Use and Disclosure of PHI received from, or created or received by, the Business Associate on behalf of, the Plan available to the Secretary for purposes of determining compliance with the HIPAA Privacy Rule;

(x) If feasible, return or destroy all PHI received from, or created or received by, the Business Associate on behalf of, the Plan that the Business Associate 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 Disclosures to those purposes that make the return or destruction of the information infeasible; and

(xi) Authorize termination of the contract by the Plan, if the Plan determines that the Business Associate has violated a material term of the agreement;

(xii) Notify the Plan of a Breach without unreasonable delay (but in no event later than 60 days) after discovery of the Breach (in accordance with the relevant requirements of 45 C.F.R. Section 164.410);

(xiii) Comply with the applicable requirements of 45 C.F.R. Section 164.502(e) for any Use or Disclosure of PHI to a subcontractor in the same manner that the Plan must comply with those requirements for contracts or other arrangements with the Business Associate.

B. **Noncompliance by a Business Associate**. The Plan is not in compliance with the HIPAA Privacy Rule relating to the Disclosure of PHI to a Business Associate if the Plan knows of a pattern of activity or practice of the Business Associate that constitutes a material breach or violation of the Business Associate's obligation under the agreement or other arrangement with the Plan, unless the Plan took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the agreement, if feasible or, if termination is not feasible, reported the problem to the Secretary.

VII. **Prohibited Uses and Disclosures**. The Plan is prohibited from making the following Uses and Disclosures of PHI:

A. Use and Disclosure of Genetic Information for underwriting purposes, which include:

1. Determining eligibility for benefits under the Plan;

2. Computing premium or contribution amounts under the Plan;

3. The application of any preexisting condition exclusion under the Plan; and

4. Other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits.

Underwriting purposes do not include determinations of medical appropriateness where an Individual seeks a benefit under the Plan.

B. Except with an Authorization pursuant to of Article III, Section V of this Policy, the Plan is prohibited from selling PHI where the Plan directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI. A sale of PHI does not include Disclosures of PHI:

1. For public health purposes pursuant to Article III, Section IV(B)(9) of this Policy;

2. For research purposes pursuant to Article III, Section IV(B)(6) of this Policy;

3. For Treatment and Payment purposes;

4. For the sale, transfer, merger or consolidation of all or part of the Plan and for related due diligence;

5. To or by a Business Associate for activities that the Business Associate undertakes on behalf of the Plan, and the only remuneration provided is by the Plan to the Business Associate for the performance of such activities;

6. To an Individual pursuant to Article IV, Section II or Article IV, Section IV of this Policy;

7. As required by law pursuant to Article III, Section IV(B)(1) of this Policy;

8. For any other purpose permitted by the HIPAA Privacy Rule, where the only remuneration received by the Plan is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law.

VIII. **Other Procedures.**

A. **Mitigation of Inadvertent Disclosures of PHI.** HIPAA requires the Plan to mitigate, to the extent practicable, any harmful effects that the Plan knows of a Use or Disclosure of PHI in violation of this Policy or HIPAA by a Workforce Member or a Business Associate or as a result of a Breach of Unsecured PHI. If you become aware of a Disclosure of PHI that is not in compliance with this Policy or HIPAA, immediately notify the Privacy Official, securityincident.im@pg.com and the Band III Director, NA Health & Wellness My P&G Services & US Benefits Delivery or if related to South Boston On-Site Medical Plan, the Band III Director Boston Site Medical Leader, so that the appropriate steps to mitigate the harm to the Individual can be taken. If you do not know who the Privacy Official, Band III Manager, NA My P&G Services & US Benefits Delivery (or equivalent) and or the Band III Director Boston Site Medical Leader are, you can email corporateprivacy.im@pg.com for this contact information.

B. **Breach Notification Procedures**. If the Plan or its Business Associate discovers a Breach of Unsecured PHI, the Plan and Business Associates must comply with the requirements of the HITECH Act and its implementing regulations to provide notification to affected Individuals, HHS, and the media (when required) and the Breach Notification Procedures (as further detailed in Article IX of this Policy).

C. **Requests for Disclosure of PHI from Spouses, Family Members, and Friends**. The Plan will not Disclose PHI to family and friends of an Individual except as required or permitted by HIPAA. Generally, a valid Authorization is required before another party, including spouse, family member or friend, will be able to access PHI.

If the Plan receives a request for Disclosure of an Individual's PHI from a spouse, family member, or personal friend of an Individual, and the spouse, family member, or personal friend is either (1) the parent of the Individual and the Individual is a minor child; or (2) the personal representative of the Individual, then follow the Verification Procedures for verifying the identity of a minor Individual's parent or an Individual's personal representative (*see* Article IV, Section VI).

Once the identity of a parent or personal representative is verified, then follow the procedures for granting or denying the request set forth in Article IV of this Policy.'

All other requests from spouses, family members, and friends must be authorized by the Individual whose PHI is involved.

D. **No Disclosure of PHI for Non-Health Plan Purposes**. The Plan may not Use or Disclose PHI for the payment or operations of the Company's "non-health" benefits (e.g., disability, workers' compensation, life insurance, etc.), unless the participant has provided a valid Authorization for such Use or Disclosure or such Use or Disclosure is required by applicable state law and particular requirements under HIPAA are met.

ARTICLE IV
INDIVIDUAL RIGHTS

HIPAA gives Individuals 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 Individuals may request to have their PHI amended, and that they are entitled to an accounting of certain types of Disclosures. Individuals also have the right to receive adequate notice of the Plan's privacy practices, as required under HIPAA. To comply with these HIPAA requirements, Workforce Members must follow this Policy with respect to PHI in the Plan's control. Third-party administrators and other Business Associates may follow their own HIPAA-compliant policies and procedures to comply with participants' Individual Rights under HIPAA.

I. **Right to Notice of Privacy Practices**. Individuals have a right to receive adequate notice, as provided in Article V of this Policy, of the Uses and Disclosures of PHI that may be made by the Plan and of the Individual's rights and the Plan's legal duties with respect to PHI.

II. **Right to Access PHI**.

A. **Policy**. Individuals have the right to access, inspect and obtain copies of their PHI that the Plan (or its Business Associates) maintains in Designated Record Sets, except for psychotherapy notes and information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding, and to request that such information be provided in the form and format requested. If the PHI that is the subject of a request is maintained electronically, Individuals may request a copy of such information to be provided in an electronic format. Individuals also may request that the Plan send a copy to a designated third party, provided that such request is made as set forth below. An access request must be made in writing (unless the Plan fails to inform the Individual of such requirement, via the Notice of Privacy Practices or otherwise), in which case the request may be made orally. The Plan will provide access to PHI in accordance with HIPAA and the below procedures for complying with an Individual's request for access.

B. **Procedures**. Upon receiving a request in writing from an Individual (or from a minor's parent or an Individual's personal representative) for access, inspection and/or a copy of an Individual's PHI, the Plan must take the steps set forth below. The Privacy Official, or its designee(s), must respond to the request by providing the information or denying the request within 30 days. If the requested PHI cannot be accessed within the 30-day period, the deadline may be extended for 30 days by providing written notice to the Individual within the original 30-day period of the reasons for the extension and the date by which the Plan will respond. The Plan may have only one such extension of time on a request for access.

1. Follow the procedures for verifying the identity of the Individual (or parent or personal representative) set forth in the Verification Procedures (*see* Article IV, Section VI).

2. Review the request to determine whether the PHI requested is held in the Individual's Designated Record Set.

3. Review the request to determine whether the request may be granted or denied. An Individual's request may be denied under certain circumstances identified in § 164.524 of the HIPAA Privacy Rule as follows:

   (i) **Unreviewable Grounds for Denial.** The Plan may deny certain requests to access PHI without providing the Individual an opportunity to review the denial, including requests to access (i) psychotherapy notes; (ii) information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or legal proceeding; (iii) made by inmates in certain circumstances; (iv) PHI obtained from an entity other than a health care provider under a promise of confidentiality, where the requested access would be reasonably likely to reveal the source of the information; and (v) information compiled during research when the Individual has agreed to denial of access when consenting to participate in the research.

   (ii) **Reviewable Grounds for Denial.** The Plan may deny certain requests to access PHI, provided the Plan gives the Individual the opportunity to have such denial reviewed by a licensed health care professional who is designated by the Plan to act as a reviewing official and who did not participate in the original decision to deny, in the following circumstances:

      (a) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or of another person;

      (b) The PHI refers to another person (other than a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

      (c) The access is requested by a personal representative and a licensed professional health care professional has determined, in the exercise of professional judgment, that access by such personal representative is reasonably likely to cause substantial harm to the individual or another person.

4. If the request is denied, a notice of denial written in plain language must be provided to the Individual, containing: (1) the basis for the denial; (2) a statement of the Individual's right to request a review of the denial, if applicable, and how to request such a review; and (3) a statement of how

the Individual may file a complaint concerning the denial and a description of how, where and to whom (e.g., the Plan's Privacy Official, Secretary of HHS) the Individual may file such complaint. All notices of denial must be prepared or approved by the Band III Director, NA Health & Wellness My P&G Services & US Benefits Delivery (or equivalent) or if related to South Boston On-Site Medical Plan, the Band III Director Boston Site Medical Leader. If access to some but not all of the PHI requested by the Individual is denied, access to the PHI that is not subject to the denial shall be provided in accordance with requirements below.

5. If the request is granted, the requested information shall be provided in accordance with the following requirements:

   (i) The access requested by the Individual, including inspection or obtaining a copy of the PHI, or both, shall be provided.

   (ii) Access shall be provided in the form or format requested by the Individual, if readily producible in the form or format requested, or, if not, in a readable hard copy form or such other form or format as agreed by the individual and the Plan.

   (iii) Notwithstanding subsection (ii), above, if the form or format requested is electronic and the PHI subject to the request is electronically maintained in one or more Designated Record Sets, the Plan must provide the Individual with access to the PHI in the electronic form and format requested by the Individual if it is readily producible in the electronic form or format requested; or, if not, provide the information in a readable electronic form or format (such as a text-based PDF), as agreed to by the Plan and the Individual.

   (iv) Notwithstanding subsections (i), (ii) and (iii) above, a summary or explanation of the requested PHI may be provided in lieu of providing access to the PHI if the Individual agrees in advance to such summary or explanation. A fee may be charged for such summary or explanation only if the Individual agrees to the fee in advance.

   (v) The Individual shall be provided access within the applicable time period under Article IV, Section II(B) of this Policy. Individuals have the right to receive a copy of their PHI by mail or by e-mail or can come in and pick up a copy. Individuals also have the right to come in and inspect the information at a time and place convenient for the Plan and the Individual.

   (vi) If the Individual requests that the information be sent to a third party, provide the information to the third party, provided that the Individual (a) makes the request in writing, (b) clearly designates

the third party (including clearly identifying the third party and where the requested information is to be sent), and (c) signs the request.

(vii) A reasonable fee for copies, explanations or summaries of the requested PHI may be charged, provided that the fee is limited to the cost of copying (including labor); supplies for creating the paper copy or electronic media if the Individual requests the electronic copy be provided on portable media; postage (if the Individual requested to have the information mailed); and preparation of the explanation or summary, if any, except as provided in subsection (iii), above.

6. The Plan must document the Designated Record Sets that are subject to access by Individuals and the titles of persons or offices responsible for receiving requests for access by Individuals in accordance with Article VIII of this Policy, "Documentation, Maintenance and Destruction of PHI."

III. **Right to Amend PHI**.

A. **Policy**. Individuals have the right to request to have their PHI amended, and the Plan will consider requests to amend PHI that are submitted in writing by participants (unless the Plan fails to inform the individual of such a requirement, via the Notice of Privacy Practices or otherwise, in which case the request may be made orally) in accordance with the following procedures for complying with an Individual's request for amendment of PHI.

B. **Procedures**. Upon receiving a request from an Individual (or a minor's parent or an Individual's personal representative) for amendment of an Individual's PHI held in a Designated Record Set, the Plan must take the steps set forth below.

1. The Plan must respond to the request within 60 days by informing the Individual in writing that the amendment will be made or that the request is denied. If the determination cannot be made within the 60-day period, the deadline may be extended for 30 days by providing written notice to the Individual within the original 60-day period of the reasons for the extension and the date by which the Plan will complete its action on the request. The Plan may have only one such extension of time on a request for an amendment.

2. Follow the procedures for verifying the identity of the Individual (or parent or personal representative) set forth in the Verification Procedures (*see* Section VI of this Article).

3. Review the amendment request to determine whether the PHI at issue is held in the Individual's Designated Record Set. If not, the Plan may deny the request as set forth below.

4. Review the request for amendment to determine whether the information would be accessible under an Individual's right to access. If not, the Plan may deny the request as set forth below.

5. Review the request for amendment to determine whether the amendment is appropriate—that is, determine whether the information in the Designated Record Set is accurate and complete without the amendment. If not, the Plan may deny the request as set forth below.

6. Review the request for amendment and determine whether the PHI or record that is subject of the request was created by the Plan. If not, the Plan may deny such request as set forth below, unless the Individual provides a reasonable basis to believe that the originator of PHI is no longer available to act on the requested amendment.

7. When an amendment is accepted, (1) make the change in the Designated Record Set (by, at a minimum, identifying the affected records and appending or otherwise providing a link to the location of the amendment), (2) provide appropriate notice to the Individual and all persons or entities listed on the Individual's amendment request form that the amendment was made, (3) obtain the individual's identification of and agreement to have the Plan notify the relevant persons that have received the PHI, and (4) notify the persons identified by the Individual as needing the amendment and persons/entities (including Business Associates) who are known to have the particular record and who may rely or could foreseeably rely on the uncorrected information to the detriment of the Individual. The Plan also shall amend PHI in accordance with a notice from another entity subject to the HIPAA Privacy Rule that the other entity has amended the PHI in accordance with the HIPAA Privacy Rule.

8. When an amendment request is denied, the following procedures apply:

    - A Denial Notice (if related to PHI that Workforce members have control over) must be approved by the Director, U.S. Health & Wellness Benefits Delivery (or equivalent) and if related to South Boston On-Site Medical Plan, the Band III Director Boston Site Medical Leader and contain: (i) the basis for the denial; (ii); information about the Individual's right to submit a written statement disagreeing with the denial and how to file such a statement; (iii) an explanation that the Individual may (if he or she does not file a statement of disagreement) request that the request for amendment and its denial be included in future Disclosures of the information; and (iv) a statement of how, to whom and where the Individual may file a complaint concerning the denial (e.g., the Plan's Privacy Official and/or the Secretary of HHS).

- Following the denial, the Individual may submit to the Plan a written statement of disagreement. The Privacy Official, or its designee(s), may reasonably limit the length of such statement. The Plan also may prepare a written rebuttal to the Individual's statement of disagreement, a copy of which shall be provided to Individual. If the Individual files a statement of disagreement, any subsequent Disclosure of PHI to which the request for amendment relates must include' the Individual's statement of disagreement and the Company's rebuttal/response to such statement of disagreement, if any. If the Individual has not submitted a written statement of disagreement, include the Individual's request for amendment and its denial with any subsequent Disclosure of the PHI only if the Individual has requested such action. Such documents may be transmitted separately if the Disclosure is made in a standard transaction under part 162 of the HIPAA Privacy Rule that does not permit the documents to be included in the Disclosure.

9. The Plan shall amend PHI in accordance with a notice from another entity subject to the HIPAA Privacy Rule that the other entity has amended the PHI in accordance with the HIPAA Privacy Rule.

10. The Privacy Official is responsible for recording, processing, and retaining requests for amendments as contemplated by Article VIII of this Policy.

IV. Right to Accounting of Disclosures of PHI.

A. **Policy**. Individuals have the right to obtain an accounting of certain Disclosures of his or her own PHI. At the Individual's written request and in accordance with the procedures below for processing requests for an Accounting of Disclosures of PHI, the Plan shall provide the Individual with an accounting of certain Disclosures by the Plan of such Individual's PHI made during the period requested but no more than six years prior to the date of the request.

B. **Procedures for Processing Requests for an Accounting of Disclosures of PHI**. Upon receiving a request from an Individual (or a minor's parent or an Individual's personal representative) for an accounting of Disclosures, the Plan must take the steps set forth below.

1. The Plan must respond to the request within 60 days by providing the accounting (as described in more detail below), or informing the Individual that there have been no Disclosures that must be included in an accounting (see the list of exceptions to the accounting requirement, below). If the accounting cannot be provided within the 60-day period, the deadline may be extended for 30 days by providing written notice to the Individual within the original 60-day period of the reasons for the extension and the date by

which the Plan will respond. The Plan may have only one such extension of time for action on a request for an accounting.

2. Follow the procedures for verifying the identity of the Individual (or parent or personal representative) set forth in the Verification Procedures (*see* Article IV, Section VI).

3. The Plan may not charge a fee for the first accounting in a 12-month period. If the Individual requesting the accounting has already received one accounting within the 12-month period immediately preceding the date of receipt of the current request, prepare a notice to the Individual informing him or her that a fee for processing will be charged and provide the Individual with a chance to withdraw the request.

4.

5. The accounting must include Disclosures (but not Uses) of the requesting Individual's PHI made by Plan and its Business Associates during the period requested by the Individual up to six years prior to the date of the request.

6. (i)The accounting must include the following information for each reportable Disclosure of the Individual's PHI:

    - the date of Disclosure;
    - the name (and if known, the address) of the entity or person to whom the information was Disclosed;
    - a brief description of the PHI Disclosed; and
    - a brief statement explaining the purpose for the Disclosure that reasonably informs the Individual of the basis for the Disclosure. (The statement of purpose may be accomplished by providing a copy of the written request for Disclosure, when applicable, or when required by the Secretary of HHS for compliance investigations.)

    (ii) If multiple Disclosures have been made to the same person or entity for a single purpose or pursuant to a single Authorization, the accounting may, with respect to such multiple Disclosures, provide:

    - the information required under subsection (i) for the first of such Disclosures;
    - the frequency, periodicity, or number of the Disclosures made; and

- the date of the last of such Disclosures during the accounting period.

7. The accounting does not have to include Disclosures made:

   - to carry out Treatment, Payment and Health Care Operations;
   - to the Individual about his or her own PHI;
   - incident to an otherwise permitted or required Use or Disclosure under the HIPAA Privacy Rule;
   - pursuant to an Individual's Authorization;
   - to persons involved in the Individual's care or payment for the Individual's care or for certain other notification purposes;
   - for specific national security or intelligence purposes;
   - to correctional institutions or law enforcement when the Disclosure was permitted without an Authorization; and
   - as part of a Limited Data Set.

8. An Accounting of Disclosures to a health oversight agency or a law enforcement official shall be temporarily suspended for a period as requested by such health oversight agency or law enforcement if:

   - Such agency or official provides the Plan a written statement that such accounting to the Individual would reasonably be likely to impede the agency's activities and specifying the time for which such a suspension is required; or
   - Such agency's or official's request is oral and the Plan documents the statement (including the agency's or official's identity), and temporarily suspends the Individual's accounting consistent with such statement for a period no longer than 30 days from the date the agency or official made its request, unless a written statement as described above is provided within such 30-day period.

9. The Plan must document the information required to be included in an accounting for Disclosures, the written accounting provided to the Individual, and the titles of the persons or offices responsible for receiving and processing requests for an accounting by Individuals.

C. **Fees**. The Plan must provide the first accounting to an Individual in any 12-month period without charge. The Plan may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same Individual within the 12-month period, provided that the Plan informs the Individual in advance of the fee and provides the Individual with an opportunity to withdraw or modify the request for subsequent accounting in order to avoid or reduce the fee.

D. **Electronic Health Records.**

1. If the Plan uses or maintains Electronic Health Records, Disclosures through an Electronic Health Record to carry out Treatment, Payment, or Health Care Operations must be accounted for as described in Article IV, Section IV (B)(6) of this Policy.

2. An Individual shall have a right to receive an accounting of Disclosures of PHI contained in Electronic Health Records made in the three years prior to the date on which the accounting is requested.

3. In response to a request from an individual for an accounting of Disclosures of Electronic Health Records, the Plan may elect to provide either:

(i) An accounting as described in Article IV, Section IV (B)(6) of this Policy for Disclosures of PHI made by the Plan and any Business Associates acting on its behalf; or

(ii) An accounting of Disclosures made by the Plan and a list of all Business Associates acting on behalf of the Plan, including contact information for such Business Associates.

E. **Documentation**. The Plan must document and retain the documentation of the information required to be included in an accounting, the written accounting provided to an Individual under this Article IV, Section IV and the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

V. Right to Request Privacy Protection on the Plan's Use and Disclosure of certain PHI.

A. **Policy**. The Plan shall permit Individuals to request, in writing, restrictions on the Plan's Use or Disclosure of PHI to carry out Treatment, Payment or Health Care Operations and restrictions on the Plan's Use or Disclosure of PHI to family members, other relatives, close personal friends or other persons involved in the Individual's care or payment for that care, or for disaster relief purposes. Except as detailed below, the Plan is not required to agree to these restrictions. The Plan also shall permit Individuals to request (in writing) and receive communications of PHI by alternative means or at alternative locations (e.g., to be called only at work, instead of home) if the request is reasonable and the Individual clearly states that any such Disclosure of all or part of that information could endanger the Individual.

The Plan must comply with the requested restriction if:

1. Except as otherwise required by law, the Disclosure is to a Health Plan for purposes of carrying out Payment or Health Care Operations (and is not for purposes of carrying out Treatment); or

2. The PHI pertains solely to a health care item or service for which the health care providers involved has been paid out of pocket in full.

Apart from these specified requested restrictions, the Plan is not required to agree to a requested restriction.

B. **Procedures**.

1. **Request for Confidential Communications**. Upon receiving a request in writing from an Individual (or a minor's parent or an Individual's personal representative) to receive communications of PHI by alternative means or at alternative locations, the Plan must take the following steps:

(i) Follow the procedures for verifying the identity of the Individual (or parent or personal representative) set forth in the Verification Procedures (*see* Article IV, Section VI).

(ii) Determine whether the request contains a statement that Disclosure of all or part of the information to which the request pertains could endanger the Individual.

(iii) Requests for confidential communications must be honored by the Plan if the Individual states that Disclosure of all or part of that information could endanger the Individual.

(iv) If a request will not be accommodated, the Plan must contact the Individual in person, in writing, or by telephone to explain why the request cannot be accommodated.

(v) Requests and their dispositions must be documented in accordance with Article VIII, "Documentation, Maintenance and Destruction of PHI."

2. **Requests for Restrictions on Use and Disclosure.** Upon receiving a written request from an Individual (or a minor's parent or an Individual's personal representative) for restriction on Use or Disclosure of an Individual's PHI, the Plan must take the following steps:

(i) Follow the procedures for verifying the identity of the Individual (or parent or personal representative) set forth in the Verification Procedures (*see* Article IV, Section VI).

(ii) The Plan should determine whether to honor requests.

(iii) If the request will not be accommodated, the Plan must contact the Individual in person, in writing, or by telephone to explain why the request cannot be accommodated. No requested restriction is valid to the extent it would prevent an accounting or access, as provided in this Article IV.

(iv) If the request will be accommodated, the Plan must comply with the request, except in the event that the PHI is necessary to provide emergency treatment to the Individual, provided that the Plan requests that the health care provider providing the emergency treatment not further Use or Disclose the information.

(v) Once granted, a restriction requested by the Individual may be terminated if the Individual agrees to the termination in writing or if the Individual agrees orally to the termination and such oral agreement is documented. The Plan also may terminate a restriction with respect to PHI received after it informs the Individual that it is terminating the restriction.

(vi) All Business Associates that may have access to the Individual's PHI must be notified of any agreed-to restrictions and terminations of restrictions.

(vii) Requests and their dispositions must be documented in accordance with Article VIII, "Documentation, Maintenance and Destruction of PHI."

VI. **Verification Procedures**.

A. **Policy**. The Plan must take steps to verify the identity of individuals who request access to PHI and verify their authority to have access to PHI, if the identity or authority of such person is not known.

B. **Procedures**. Separate procedures are set forth below for verifying identity and authority, depending on whether the request is made by the Individual, a parent seeking access to the PHI of his or her minor child, a personal representative, or a public official seeking access.

1. **Request Made by Individual**. When an Individual requests access to his or her own PHI, the Plan should follow these steps:

- Request a form of identification from the Individual. The Plan may rely on a valid driver's license, passport or other photo identification issued by a government agency.

- Verify that the identification matches the identity of the Individual requesting access to the PHI. If you have any doubts as to the validity or authenticity of the identification

provided or the identity of the individual requesting access to the PHI, contact the Privacy Official.

- Make a copy of the identification provided by the Individual and file it with the Individual's Designated Record Set.

- Disclosures must be documented in accordance with Article VIII of this Policy, "Documentation, Maintenance and Destruction of PHI."

2. **Request Made by Parent Seeking PHI of Minor Child**. When a parent requests access to the PHI of the parent's minor child, the Plan should follow these steps:

   - Seek verification of the person's relationship with the child. Such verification may take the form of confirming enrollment of the child in the parent's plan as a dependent.

   - Disclosures must be documented in accordance with Article VIII of this Policy, "Documentation, Maintenance and Destruction of PHI."

3. **Request Made by Personal Representative**. When a personal representative requests access to an Individual's PHI, the Plan should follow these steps:

   - Require a copy of a valid power of attorney, guardianship papers, or administrator/executor documents (or other documentation—requirements may vary state-by-state) before releasing any PHI to the personal representative. If there are any questions about the validity of the documentation provided, the Plan should seek review by the Privacy Official.

   - Make a copy of the documentation provided and file it with the Individual's Designated Record Set.

   - Disclosures must be documented in accordance with Article VIII of this Policy, "Documentation, Maintenance and Destruction of PHI."

4. **Request Made by Public Official**. If a public official requests access to PHI, and if the request is for one of the purposes set forth in in Article III with respect to mandatory Disclosures of PHI or permitted Disclosures of PHI, the Plan should follow these steps to verify the official's identity and authority):

- If the request is made in person, request presentation of an agency identification badge, other official credentials, or other proof of government status. Make a copy of the identification provided and file it with the Individual's Designated Record Set.

- If the request is in writing, verify that the request is on the appropriate government letterhead.

- If the request is by a person purporting to act on behalf of a public official, request a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

- Request a written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority. If the individual's request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, contact the Privacy Official.

- Obtain approval for the Disclosure from the Privacy Official.

- Disclosures must be documented in accordance with Article VIII , "Documentation, Maintenance and Destruction of PHI."

5. **Requester is Not Known.** If the identity or authority of the requestor is not known, the following procedures must be followed.

(i) Workforce Members must exercise professional judgment in making Disclosures of PHI. In the event a Workforce Member is uncertain whether the requestor is acting in good faith, the member should consult the Privacy Official prior to Disclosing PHI.

(ii) To verify his or her identity, the requestor must:

(a) Provide his or her name and relationship to the individual who is the subject of the PHI;

(b) Have a general knowledge of the information requested; and

(c) Know at least two of the following pieces of information about the individual who is the subject of the PHI:

- Social Security number;
- Employee identification number;
- Home address;
- Birth date;
- Telephone number;
- The Plan number; and
- Date of service.

6. **Authority.** Workforce Member may rely, if reasonable under the circumstances, on any of the following to verify the requestor's authority:

   (i) A written statement of the legal authority under which the PHI is requested;

   (ii) If a written statement of the legal authority would be impracticable, an oral statement of such legal authority; or

   (iii) If a request is made pursuant to legal process, the warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

ARTICLE V
NOTICE OF PRIVACY PRACTICES

I. **Policy**

Any participant enrolled in the Plan is entitled to notice of the Uses and Disclosures of his or her PHI that may be made by the Plan and the participant's rights and the Plan's legal duties with respect to the PHI.

II. **Procedures**:

A. **Benefits Provided Solely Through Insurance Contract**. In the event health care benefits are provided solely through an insurance contract, the health insurance issuer or HMO is responsible for providing notice to individuals receiving benefits under the Plan from such health insurance issuer or HMO. The Plan's obligation to maintain a copy of the notice depends upon the extent to which the Plan is involved in the creation or receipt of PHI.

1. **The Plan Creates or Receives More than Limited Protected Health Information.** If the Plan provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and creates or receives PHI *in addition to* Summary Health Information or information on whether a participant is participating in the Plan or is enrolled in or has disenrolled from the health insurance issuer or HMO, the Plan shall maintain a notice and provide such notice upon request to any person. The Plan has no obligation to otherwise deliver notice.

2. **The Plan Creates or Receives Limited Protected Health Information**. If the Plan provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive PHI other than Summary Health Information or information on whether an individual is participating in the Plan or is enrolled in or has disenrolled from the health insurance issuer or HMO, the Plan is not required to maintain a copy of or provide a notice.

B. **Required Elements of a Notice**. The Plan must provide a notice that is written in plain language and contains the following:

1. The statement as a header or prominently displayed "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY";

2. A description, including at least one example, of the types of Uses and Disclosures that the Plan is permitted to make for each of Treatment, Payment, and Health Care Operations;

3. A description of other purposes for which the Plan may Use or Disclose PHI without Consent or Authorization;

4. A statement that other Uses or Disclosures will be made only with the Individual's written Authorization and that any such Authorization may be revoked, including a specific statement that the sale, Use or Disclosure of PHI for marketing purposes or, if applicable, Use or Disclosure of psychotherapy notes requires an Authorization;

5. A statement that the Plan may Disclose PHI to the Plan Sponsor;

6. A statement explaining that the Plan may not Use or Disclose PHI that is Genetic Information for underwriting purposes;

7. A statement of the participant's rights with respect to the PHI, as contemplated by Article IV of this Policy, including, the right to request restrictions, the right to receive confidential communications, the right to inspect and copy, the right to receive an accounting of Disclosures;

8. A statement that the Plan is required by law to maintain the privacy of PHI and provide participants with notice of its legal duties and privacy practices, to abide by the terms of the notice currently in effect and to provide notice of a Breach of Unsecured PHI;

9. If the Plan intends to contact participants for fundraising, a statement that participants have the right to opt out of receiving fundraising communications;

10. A statement that reserves the Plan's right to change the terms of the notice and make the new notice effective for all protected health information that it maintains and a statement describing how it will provide Individuals with the revised notice;

11. A statement that participants may complain to the Privacy Official and the Secretary of HHS if they believe their privacy rights have been violated, a brief description of how the participant may file a complaint with the Plan and a statement that the participant will not be retaliated against for filing a complaint;

12. The name, title or office to contact for further information; and

13. The date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

C. **Timing of Notice**. The Plan shall provide notice to participants at time of enrollment for any new enrollee. In addition, Plan shall notify participants then covered no less frequently than once every three (3) years of the availability of the notice and how to obtain a copy of it. The requirement to provide notice is satisfied

by providing such notice to the named insured of a policy under which coverage is provided to the named insured and one or more dependents. If a material change is made to a Plan's current notice, the change or an updated notice must be prominently posted on its web site by the effective date of the change. In addition, such information (and an explanation as to how to obtain a copy of the updated notice if not otherwise included) must also be included in the next annual mailing to covered Individuals. If the information is not posted to a web site, such information (and an explanation as to how to obtain a copy of the updated notice if not otherwise included) must be provided to all covered Individuals within 60 days of the effective date of the change.

D. **Electronic Notice**

1. **Required Web Site Posting**. The Plan maintains a web site providing information about the Plan's benefits shall prominently post the Notice of Privacy Practices set forth in Appendix C on the web site and make the notice available electronically through the web site.

2. **Electronic Mail Notice Permitted**. The requirements of this Article V may be satisfied by electronic mail, if the participant agrees to electronic notice and such agreement has not been withdrawn. If the Plan knows that the electronic mail transmission failed, a paper copy of the Notice of Privacy Practices set forth in Appendix C shall be provided to the participant.

3. **Right to Paper Copy.** Regardless of any electronic provision of the Notice of Privacy Practices set forth in Exhibit G, a participant shall be entitled to obtain a paper copy of the notice upon request.

E. **Documentation**. The Plan must document compliance with the notice requirements set forth in this Article V by retaining copies of the notices issued as provided in Article VIII.

ARTICLE VI
SAFEGUARDING PHI

I. **Policy**.

The Plan Sponsor has implemented and maintains on behalf of the Plan appropriate administrative, physical and technical safeguards or "firewalls" to prevent PHI from intentionally or unintentionally being Used or Disclosed in violation of this Policy and the HIPAA requirements. Further, the Plan Sponsor and the Plan have made reasonable efforts to limit the incidental Use or Disclosure of PHI made pursuant to an otherwise permitted or required Use or Disclosure. Examples of safeguards in place are provided below.

II. **Procedures**.

The safeguards provided below will help the Plan ensure that (a) only authorized Workforce Members will have access to PHI, (b) the amount of PHI they receive satisfies the Minimum Necessary Standard described in Article VII and (c) authorized Workforce Members with access to PHI will not further Use or Disclose PHI in violation of HIPAA.

A. **Physical Safeguards**. The Plan shall maintain physical restrictions on access to hard-copy PHI on the Plan's premises and shall further restrict oral discussions involving PHI to designated areas, to the extent reasonable. The Privacy Official shall ensure that physical safeguards are erected and maintained by the Plan, including maintaining paper documents containing PHI in locked cabinets or locked file rooms to which only Workforce Members shall have access.

B. **Technical Safeguards**. Where PHI is stored or transmitted by computer, the Plan shall restrict access to e-PHI by using technical safeguards, which may include special passwords, an automatic log-off system for computers holding PHI and procedures for clearing hard drives of data.

C. **Administrative Safeguards**. The Plan shall limit access to PHI to those Workforce Members who require access to this information to carry out their duties and job responsibilities, and then only to the category of PHI to which access is needed.

The following sets forth the title or classes of Workforce Members who require and shall have access to PHI to carry out their Plan-related duties and job responsibilities; the categories of PHI to which they shall have access; and any conditions or requirements that must be satisfied before access is granted:

Workforce Member Role/Organization/Description (as of April 2022)

Role	Organization	Plan-related Duties
BTA	GBS – My P&G Services	Benefits Delivery
Band 2 Manager	GBS – My P&G Services	Benefits Delivery

Band 2 Manager	GBS – My P&G Services	Benefits Delivery
Band 3 Manager	GBS – My P&G Services	Benefits Delivery
Band 3 Manager	GBS – My P&G Services	Benefits Delivery
Band 4 Manager	GBS – My P&G Services	Benefits Delivery
Band 4 Manager	Corporate Function – Legal	Global Benefits & Taxation
BTA	GBS – My P&G Services	Benefits Market Operations
BTA	GBS – My P&G Services	Benefits Market Operations
Band 2 Manager	GBS – My P&G Services	Benefits Market Operations
Band 3 Manager	GBS – My P&G Services	Benefits Market Operations
Band 3 Manager	Corporate Function – Medical	Executive Benefits
Band 2 Manager	Corporate Function - Medical	NA Health Systems
Band 4 Manager	Corporate Function - Medical	NA Health Systems
Band 3 Manager	Corporate Function-HR	Benefits Design
Band 5 Manager	Corporate Function-HR	Benefits Design
Band 3 Manager	GBS – My P&G Services	Technical Information Security
Band 2 Manager	GBS - My P&G Services	Retiree Benefits
Band 2 Manager	Corporate Function – Legal	Privacy, Cybersecurity & IT Law
Band 3 Manager	Corporate Function – Legal	Privacy, Cybersecurity & IT Law
Band 5 Manager	Corporate Function – Legal	Global Privacy Officer
Band 1 Manager	Corporate Function – Legal	Labor & Employment Law
Band 2 Manager	Corporate Function – Legal	Labor & Employment Law
Band 3 Manager	Corporate Function – Legal	Labor & Employment Law
Band 4 Manager	Corporate Function – Legal	Labor & Employment Law

Band 2	Corporate Function – Information Security	Incident Response
Band 3	Corporate Function – Information Security	Incident Response
Band 2 Manager	GBS – My P&G Services	Benefits Delivery
Band 3 Manager	GBS – My P&G Services	Benefits Delivery
BTA	GBS – My P&G Services	Benefits Market Operations

The Workforce Members described above shall comply with the Policy, including Article III describing the restrictions on Use and Disclosure of PHI. In the event that any of the Workforce Members described above fails to comply with the Policy, sanctions and/or disciplinary actions shall be imposed in accordance with the Plan Sponsor's discipline policy and applicable law, up to and including termination.

ARTICLE VII
COMPLYING WITH THE MINIMUM NECESSARY STANDARD

I. **Policy**.

The Plan is committed to ensuring the privacy and security of PHI held in connection with those programs maintained as part of the "group health plan" components of the Plan (*see* Appendix A for the list). Although participant information must be available to the Plan in order for the Plan to carry out its necessary functions, in the process of undertaking such functions, Workforce Members should avoid Using, Disclosing or requesting more PHI than the Minimum Necessary. To support the Plan's commitment to participant confidentiality, any Use, Disclosure or request by the Plan must be limited to a Limited Data Set and the minimum amount of PHI necessary to accomplish the intended purpose of the Use, Disclosure, or request, as required under 45 C.F.R. § 164.502(b) and § 164.514(d). In general, unless and until regulations are issued by the Secretary of HHS, any such Use, Disclosure or request will be limited to a Limited Data Set unless more information is needed, in which case, the Use, Disclosure or request will be limited to the Minimum Necessary.

II. **Procedures**.

A. Workforce Members must follow the procedures detailed in this Policy to ensure that only the minimum amount of PHI necessary to accomplish the intended purpose of a Use or Disclosure is actually Used or Disclosed. Workforce Members must request only the minimum amount of PHI necessary to accomplish the intended purpose of any request.

B. **Exceptions:** The Minimum Necessary Standard does not apply to any of the following:

- Disclosures to or requests by a health care provider for Treatment;
- Uses or Disclosures made to the Individual who is the subject of the PHI Disclosed;
- Uses or Disclosures made pursuant to a valid Authorization;
- Disclosures made to HHS pursuant to the compliance and enforcement provisions of the HIPAA Privacy Rule;
- Uses or Disclosures required by law; and
- Uses or Disclosures required to comply with the HIPAA Privacy Rule.

C. **Access to PHI**. The Plan shall make reasonable efforts to limit access to only to those Workforce Members or classes of Workforce Members with respect to the category or categories of PHI designated. Such Workforce Members or classes of Workforce Members are limited to those who need access to PHI to carry out their

duties for the Plan. A Workforce Member or class of Workforce Members may access the PHI designated for such Workforce Member or Class of Workforce Members only if the Workforce Member satisfies the applicable conditions for such access, if any.

D. **Routine and Recurring Disclosures**. For each type of Disclosure made on a routine and recurring basis (e.g., assisting participants in the resolution of health care claims) ,the Plan shall identify the types of PHI to be Disclosed, the types of persons who may receive the PHI, the conditions that would apply to such access, and the standards for Disclosures to routinely hired types of Business Associates. the Plan must create and implement policies and procedures for each specific routine and recurring Disclosure that limits the amount of PHI Disclosed to the minimum amount necessary to accomplish the purpose of the Disclosure.

E. **Other Disclosures**. For all other non-routine Uses and Disclosures of PHI, such as related to judicial and administrative proceedings, will be considered on a case-by-case basis and must be approved by the Privacy Official or its delegate.. The Privacy Official or his or her delegate shall use the following criteria when making case-by-case determinations for non-routine Uses and Disclosures of PHI:

1. Is there a legitimate and reasonable need for any or all of the PHI proposed to be Used or Disclosed?

2. Can the Use or Disclosure be satisfied using De-Identified Health Information?

3. If De-Identified Health Information cannot be used, is the amount of information proposed to be Used or Disclosed limited to only the minimum amount of PHI necessary to perform the Plan administration function?

In responding to a request for PHI, the Plan may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the Minimum Necessary for the stated purpose when:

1. Making disclosures to public officials when permitted under the HIPAA Privacy Rule, if the public official represents that the information requested is the Minimum Necessary for the stated purpose;

2. The information is requested by another entity subject to the HIPAA Privacy Rule;

3. The information is requested by a professional who is a member of the Plan Workforce or is a Business Associate of the Plan for the purpose of providing professional services to such Plan, if the professional represents that the information requested is the Minimum Necessary for the stated purpose; or

4. Documentation or representations that comply with the relevant provisions of the HIPAA Privacy Rule have been provided by a person requesting the information for research purposes.

F. **Requests for PHI by the Plan**

1. **Requests for PHI from Other Entities Subject to HIPAA Privacy Rule.** Any request for PHI by another Covered Entity, including another component of the Plan, must be limited to the Minimum Necessary.

2. **Routine and Recurring Requests**. For requests for PHI made on a routine and recurring basis, the Plan should identify the information that is necessary for the purpose of the requested Disclosure and create a policy that limits each request to the minimum amount necessary to accomplish the purpose of the Disclosure. For all other requests for PHI, the Plan should contact the Privacy Official, who will ensure that the amount of PHI Disclosed is the Minimum Necessary.

3. **Other Requests.** Requests for PHI, other than the types of routine and recurring requests described above, must be reviewed by the Privacy Official, or his or her delegate, prior to being made to determine that the PHI sought is limited to the information reasonably necessary to accomplish the purpose for which the request is made. Non-routine requests for PHI will be considered on a case-by-case basis and must be approved by the HIPAA Privacy Official. The HIPAA Privacy Official shall use the following criteria when making case-by-case determinations for non-routine requests for Protected Health Information:

(i) Is there a legitimate and reasonable need for any or all of the PHI proposed to be collected?

(ii) If De-Identified Health Information cannot be used, is the amount of information proposed to be Used or Disclosed limited to only the minimum amount of PHI necessary to perform the Plan administration function?

G. **Restriction on Entire Medical Records**. The Plan may not Use, Disclose or request an entire medical record, unless the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the Use, Disclosure or request.

H. **De-Identified Health Information.** If the purpose of a Use or Disclosure can be met by Using De-Identified Health Information, it is the policy of the Plan to first de-identify the PHI before Using or Disclosing it.

ARTICLE VIII
DOCUMENTATION, MAINTENANCE AND DESTRUCTION OF PROTECTED HEALTH INFORMATION

I. **Policy**. The Plan shall retain the documentation listed in this Article for six years from the later of the date it was created or the date it was last in effect (unless other applicable law requires a longer retention period), and shall ensure that any documentation containing PHI is thereafter adequately destroyed or maintained in a manner that limits its Use or Disclosure.

II. **Rules Regarding Maintenance**. The Plan shall retain the documentation in Section IV of this Article for six years from either the date it was created or the date it was last in effect, whichever is later.

III. **Procedure**.

A. **Documents Retained in Electronic Form**. If documents containing PHI are retained in electronic form, the Privacy Official shall consult with the appropriate technical personnel to ensure:

1. The recordkeeping system has reasonable controls designed to ensure the integrity, accuracy, authenticity and reliability of the electronic records;

2. The electronic records are maintained in reasonable order, in a safe and accessible place and are capable of being readily inspected or examined; and

3. Adequate records management systems are established and implemented to ensure that documents are labeled adequately and stored securely, backup electronic copies are made, and paper copies are kept for records that cannot be clearly, accurately and completely transferred to electronic media.

In the event that the documents are maintained electronically by a third party, the Privacy Official shall ensure that such third party complies with these requirements.

B. **Destruction and Storage**. The Plan's procedures for maintenance and destruction of records may include the following:

1. Shredding documents that can be destroyed consistent with the HIPAA Privacy Rules if there is no possibility that those documents may be needed for litigation defense or other purposes; and

2. Marking records that contain PHI prior to storage of those records so that employees are aware that PHI contained in those records shall remain subject to the HIPAA Privacy Rules and this Policy for as long as those records are retained.

IV. **Documentation to be Retained**. In accordance with the HIPAA Privacy Rule and this Policy, the Plan or the Privacy Official on behalf of the Plan shall inform Workforce Members and establish a system to document and retain the following documents as set forth in this Article VIII:

A. Each self-insured group health and welfare plan in the U.S. sponsored by the Plan Sponsor to which HIPAA and this Policy applies, as set forth in Appendix A.

B. Workforce Members who need access to PHI to carry out their duties, and the categories of PHI to which access is needed.

C. Designation of the Privacy Official and any his or her designees responsible for implementing the Plan's policies and procedures;

D. Prior versions and current version of this Policy, including documentation of any changes or revisions made to this Policy as contemplated in Article II of this Policy;

E. Documentation of any Breaches, including documentation related to the discovery (reporting of the Breach), investigation, determination of whether Unsecured PHI was involved, Risk of Harm Assessments, and notifications provided to affected Individuals, the Secretary of HHS, the media and any other third parties (*see* Article IX);

F. All signed Authorizations used by the Plan to authorize the release of PHI(if information is obtained directly from a Business Associate, the Business Associate shall retain the Authorization);

G. Copies of the Plan's Notice of Privacy Practices issued by the Plan to date, including revisions made and the Notice currently in effect;

H. The Designated Records Sets that are subject to access by the Individuals as contemplated in Article IV of this Policy.

I. Documentation regarding the requests made to exercise the following individual rights (as contemplated in Article IV and related forms), including the titles of persons or offices responsible for receiving and processing such requests made by Individuals, copies of the requests, determination and/or disposition of such requests:

1. Right to request amendment of PHI;

2. Right to request an accounting of Disclosures of PHI;

3. Right to request access, inspection and obtain copies of PHI;

4. Right to request restrictions on Uses and Disclosures of PHI; and

5. Right to request confidential communications of PHI.

J. Records of Uses and Disclosures of PHI that are required to be accounted for under the HIPAA Privacy Rules and that must be made available to an Individual (as in Article IV);

K. All complaints with respect to the Plan's privacy practices received and the resolution of each complaint (as contemplated in Article II);

L. Records of any sanctions or disciplinary actions imposed by the Plan and/or Privacy Official in connection with a violation of HIPAA and/or this Policy (as contemplated in Article II);

M. Records on any Use and Disclosure of PHI for certain research purposes, as permitted without Authorization under the HIPAA Privacy Rules (as detailed in Article III, Section IV(B)(6));

N. Copies of signed Business Associate Agreements; and

O. Documentation of the training provided to Workforce Members as detailed in Article II.

ARTICLE IX
BREACH NOTIFICATION REQUIREMENTS AND PROCEDURES

I. **Policy**.

The HITECH Act imposed the HIPAA Breach Notification Rule, which requires Covered Entities to notify affected Individuals, the Secretary of HHS and the media (in certain instances) and take certain other actions in the event of a Breach of Unsecured PHI. The Plan shall comply with the following requirements and use the below Breach Notification Procedures ("Breach Procedures") to comply with the HIPAA Breach Notification Rule.

II. **Requirements**.

The Plan and its Business Associates should identify and respond to any suspected or known Breach. In accordance with the HITECH Act and this Policy, Business Associates are to report Breaches of Unsecured PHI to the Plan without unreasonable delay and in no case later than 60 days of discovery (except when such notice would impede a criminal investigation as provided by law).

All suspected or reported Breaches shall be notified to securityincident.im@pg.com and investigated pursuant to the Breach Procedures detailed below and the Company's Incident Response Guidelines.

Investigations shall include the principles outlined herein in addition to those outlined in the Incident Response Guidelines. The Privacy Official (or his or her delegate) shall be the process leader (the "Investigator") for the investigation.

If it is determined that a Breach of Unsecured PHI occurred, the Plan must provide notice as specified in this Policy.

III. **Procedures**.

A. **PHI that is Secured under the HITECH Guidance Standards**.

1. **Secured PHI**. PHI maintained by or on behalf of the Plan should be secured in accordance with the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable or Indecipherable to Unauthorized Individuals issued by the Secretary of HHS (the "HITECH Guidance Standards"). For PHI that is encrypted in accordance with the HITECH Guidance standards, the Plan and its Business Associates should keep encryption keys on a separate device from the data that they encrypt or decrypt. Note that redaction is not an acceptable form of securing paper PHI.

2. **Inapplicability of Breach Notification Rule to Secured PHI**. PHI secured in accordance with the HITECH Guidance standards ("Secured PHI") is not subject to the Breach Notification Rule requirements.

B. **Identification of Potential Breach of Unsecured PHI**.

1. **Reporting Potential Breach**. If a Workforce Member identifies a potential improper acquisition, access, Use, or Disclosure of Unsecured PHI, the Workforce Member should report the matter as soon as possible to the Privacy Official (or delegate), Band III Director, NA Health & Wellness My P&G Services & US Benefits Delivery (or equivalent) and if related to South Boston On-Site Medical Plan, the Band III Director Boston Site Medical Leader, or to one of the resources set forth in the Company's Worldwide Business Conduct Manual. If either the Band III Director, NA Health & Wellness, My P&G Services & US Benefits Delivery (or equivalent) or one of the resources set forth in the Company's Worldwide Business Conduct Manual are notified, they will forward the information to the Privacy Official (or his delegate). Contact information for the current Band III Director, NA Health & Wellness My P&G Services & US Benefits Delivery (or equivalent) and if related to South Boston On-Site Medical Plan, the Band III Director Boston Site Medical Leader, as well as other contacts mentioned in this Policy, are available by emailing corporateprivacy.im@pg.com for this information.

2. **Determination of Whether Unsecured PHI Was Involved**. The Investigator should determine whether the event indeed involved PHI that was not secured as set forth in the HITECH Guidance standards.

- If the event involved Unsecured PHI, then the Investigator should proceed to determine whether the event constitutes a Breach in accordance with this Section III.
- If the event did not involve Unsecured PHI, it should be resolved in accordance with the Company's Incident Response Guidelines. Any such event should be immediately reported to securityincident.im@pg.com.

C. **Determination of Whether the Event Constitutes a Breach under the HITECH Act**.

1. **Review of Exceptions**.

- The investigator shall verify that the incident does not fall within an exception to the definition of Breach (see Article I, definition of Breach).
- If an exception is applicable, the event shall be handled in accordance with the Incident Response Guidelines and, if applicable the Company's Security Policy with respect to Highly Restricted Information.
- If an exception does not apply, conduct the risk assessment described below ("Risk of Harm Assessment").

2. **Presumption of Breach and Compromised Standard**. Any acquisition, access, Use, or Disclosure of PHI other than those expressly permitted under HIPAA is presumed to be a Breach unless the Plan or Business Associate (as applicable) can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment. The Investigator should perform the risk assessment, including consideration of at least the following factors:

    - The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification.
    - The unauthorized person who used the PHI or to whom the PHI was Disclosed.
    - Whether the PHI was actually acquired and viewed.
    - The extent to which the risk to the PHI has been mitigated.

If the investigator can demonstrate that there is a low probability that the PHI was compromised, the event shall not constitute a Breach and shall be handled in accordance with the Incident Response Guidelines and, if applicable, the Company's Security Policy with respect to Highly Restricted Information. If the Investigator cannot demonstrate that there is a low probability that the PHI was compromised, the event will constitute a Breach of Unsecured PHI and should be reported as outlined in this Section III.

D. **Notification of Breach**.

1. **Timing of Notification; Discovery of Breach**.

    (i) A Breach of Unsecured PHI shall be treated as discovered by the Plan as of the first day that such Breach is known by the Plan. The Plan is deemed to have such knowledge if the Breach is known or, by exercising reasonable diligence, would have been known to a Workforce Member or Agent of the Plan (other than the person committing the Breach).

    (ii) A Breach of Unsecured PHI shall be treated as discovered by a Business Associate as of the first day that such Breach is known by the Business Associate. A Business Associate is deemed to have such knowledge if the Breach is known or, by exercising reasonable diligence, would have been known to an employee, officer, or other Agent of the Business Associate (other than the person committing the Breach).

2. **Timing Subject to Law Enforcement Delay**. If a law enforcement officer states to the Plan or its Business Associate that a notification, notice, or posting required under the Breach Notification Rule would impede a criminal investigation or cause damage to national security, the Plan shall delay notification as follows:

(i) If the statement is in writing and specifies the time for which a delay is required, delay the notification, notice, or posting for the time period specified by the official.

(ii) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily, but no longer than 30 days from the date of such statement, unless a written statement as described in (i) above is submitted during that time.

All timing set forth below is subject to this Timing Subject to Law Enforcement Delay section:

3. **Notify Affected Individuals**.

- If a Breach of Unsecured PHI has occurred, the Plan or its Business Associate (if applicable) shall notify each Individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or Disclosed as a result of such Breach.

- The notification shall occur without unreasonable delay, but in no event later than 60 calendar days after the discovery of the Breach of Unsecured PHI.

- The notification shall include, to the extent possible:

  - A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

  - A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

  - Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;

  - A brief description of what the Plan is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breaches; and

- The method of contacting the Band III Director, NA Health & Wellness My P&G Services & US Benefits Delivery (or equivalent) and if related to South Boston On-Site Medical Plan, the Band III Director Boston Site Medical Leader or appropriate contact for the Business Associate for questions or to learn additional information.

4. **Method of Notification**.

(i) Written Notification. Where a current address is available, written notification is required. Written notification may be provided in one or more mailings as information becomes available. Written notification must be made through one of the following means:

- First-class mail at the last known address of the Individual.
- By electronic mail if the Individual agrees to electronic notice and such agreement has not been withdrawn.
- First-class mail to the next of kin or personal representative of an affected Individual that is deceased, if the address of the next of kin or personal representative is known.

(ii) Substitute Notification when there is Insufficient or Out-of-Date Contact Information.

- When there is insufficient or out-of-date contact information for fewer than 10 affected Individuals, substitute notice may be provided by an alternative form of written notice, telephone or other means.
- In the case in which there is insufficient or out-of-date contact information for 10 or more affected Individuals, then such substitute notice shall be in the form of:
  - Either a conspicuous posting for a period of 90 days on the home page of the Plan's (or third-party administrator's) website, or conspicuous notice in major print or broadcast media in geographic areas where the Individuals affected by the Breach likely reside; and

- Include a toll-free phone number that remains active for at least 90 days where an Individual may learn whether his or her Unsecured PHI may be included in the Breach.

Substitute form of notification is not required to notify a next of kin or personal representative of a deceased Individual.

(iii) Additional Notice in Urgent Situations. If the Investigator deems a situation urgent because of possible imminent misuse of Unsecured PHI, the Plan may provide information to affected Individuals by telephone or other means, as appropriate, in addition to the previously described notification requirements.

5. **Notify the Media** (Breaches over 500 residents of a State).

- For a Breach of Unsecured PHI involving more than 500 residents of a State, the Plan shall notify the media outlets serving the State without unreasonable delay but in no case later than 60 calendar days after the discovery of the Breach.

- The content of the notification shall be the same as that provided to the affected Individuals (see above).

6. **Notify the Secretary of Health and Human Services**.

- For a Breach of Unsecured PHI involving 500 or more Individuals nationwide, the Plan shall notify the Secretary of HHS of the Breach at the same time that Individual notice is provided. Notification shall be in the form specified on HHS's website.

- For a Breach of Unsecured PHI involving less than 500 Individuals, the Plan shall maintain an annual log of such Breaches discovered during the calendar year and provide the information in such log to the Secretary of HHS no later than 60 days after the end of each calendar year. (For example, by February 28, 2022, the entity should report all Breaches of Unsecured PHI occurring in 2021.)

E. **Notification by Business Associates**.

1. **Duty to Report to the Plan**. The Plan's Business Associates are required by law to notify the Plan of Breaches of Unsecured PHI that the Business Associates discover. In these cases, the Business Associates should have

already identified the Breach as involving Unsecured PHI and compromising the security and privacy of PHI.

2. **Timing**. The Business Associate must provide notification without unreasonable delay and in no case later than 60 calendar days after the discovery of the Breach.

3. **Content**. The notification to the Plan shall include:

(i) To the extent possible, the identification of each Individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or Disclosed during the Breach; and

(ii) Any other information available at the time notification is given regarding:

- A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;
- A description of the types of Unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- Any steps Individuals should take to protect themselves from potential harm resulting from the Breach; and
- A brief description of what the Business Associate is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any further breaches.

(iii) If any of the foregoing information becomes available to the Business Associate after the date of notification, the Business Associate should promptly provide that information to the Plan.

4. **Action by the Plan.** Upon receipt of such notification, the Plan shall follow the procedures set forth in this Policy (e.g., investigation if necessary, notification and documentation), except to the extent that a Business Associate is responsible for such actions under the terms of an applicable Business Associate Agreement or by written agreement between the Plan and the Business Associate at the time of the incident.

F. **Documentation of a Breach**.

Except to the extent that a Business Associate is responsible for documenting Breaches under the terms of an applicable Business Associate Agreement, the Privacy Official (or

equivalent) should document all Breaches and their outcomes, including any actions taken in mitigation of harmful effects, written documentation of any Risk of Harm Assessments and determination made under such Risk of Harm Assessments, written documentation of notification given under the Breach Notification Rule, any sanctions or disciplinary actions levied against a Workforce Member, and any actions taken with respect to a Business Associate, Agent, or others identified as causing the Breach or being involved with the Breach.

All documentation resulting from these Procedures should be retained for at least six years from the date of creation or the last effective date, whichever is later.

G. **Administrative Requirements**.

1. **Sanctions**.

(i) Workforce Members found to have caused a Breach or failed to abide by this Policy (including these Procedures) shall be sanctioned in accordance with this Policy.

(ii) For any Breach caused by an Agent, Business Associate or any of their Agents, the Plan should take appropriate action in accordance with the terms of applicable agreements and legally available remedies.

2. **No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy.** The Plan shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against Individuals for exercising their rights or participating in any process set forth in the HIPAA Breach Notification Rule or these procedures. Further, no Individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.

3. **Additional Administrative Requirements Set Forth in this Policy**. This Policy provides additional procedures related to the Breach Notification Rule, including training requirements and complaint procedures as described in Article II of this Policy.

4. **Revisions**. The Privacy Official shall monitor revisions of the Breach Notification Rule, the HITECH Guidance, and other legal or regulatory developments relating the Breach Notification Rule and revise these procedures as necessary.

SOUTH BOSTON ON-SITE MEDICAL PLAN

Appendix A

Designation of HIPAA Hybrid Entity Health Care Components

The following Plan components are health care components of the Plan and are subject to the Plan's' HIPAA Privacy and Security Policies and Procedures, including this Policy. This list shall be amended from time to time. In the event the Plan incorporates a new component that constitutes a group health plan, as defined by HIPAA, such component shall be deemed to incorporated into the below list and shall be subject to the Plan's HIPAA Privacy Policies and Procedures (this Policy).

PROCTER & GAMBLE HEALTH AND LONG-TERM DISABILITY PLAN	MAJOR MEDICAL, PRESCRIPTION DRUG, VISION, DENTAL
PROCTER & GAMBLE RETIREE WELFARE BENEFITS PLAN	MAJOR MEDICAL, PRESCRIPTION DRUG, VISION, DENTAL
GILLETTE COMPANY RETIREE MEDICAL PLAN	MAJOR MEDICAL, PRESCRIPTION DRUG

Appendix B
Forms and Other Documents

THE PROCTER & GAMBLE COMPANY

AUTHORIZATION FOR USE AND DISCLOSURE

OF PROTECTED HEALTH INFORMATION

This authorization affects your rights to the privacy of your protected health information ("PHI"). **Please read it carefully before signing.**

The Procter & Gamble Company and its subsidiaries (collectively, the "Company") sponsor certain self-insured group health plans in the United States (collectively, the "Plan"). The Plan will not limit eligibility or enrollment in the Plan or payment or reimbursement for healthcare services on your providing authorization for the requested use or disclosure.

By signing this authorization you acknowledge and agree that:

_____

[Name or specific identification of person(s) or class of person(s), including business associates, authorized to make the requested use or disclosure. This means the person or business who will be disclosing the information]

may use or disclose the following information:

_____

[Identify the specific type of information to be used or disclosed.]

for the purpose(s) of:

_____

[Include a description of each intended use or disclosure. If the individual to whom the information pertains initiates the authorization, "at the request of the individual" may be used.]

By signing this authorization you agree that:

_____

[Name of authorized person or entity. This means the person or business who will be disclosing the information.]

may disclose your PHI to:

_____

[Name or other specific information of person(s) or entity to receive the requested use or disclosure.]

Further, by signing this authorization you acknowledge that you have been provided a copy of and have received the Plan's HIPAA Notice of Privacy Practices containing a complete description of your rights, and the permitted uses and disclosures under HIPAA.

You have the right to revoke this authorization, in writing, at any time, except to the extent that the Plan has taken action in reliance on it or, if the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy. A revocation is effective upon receipt by the Plan of a written request to revoke and a copy of the executed authorization form to be revoked at the following address:

Band III Director, Health & Wellness NA My P&G Services & US Benefits Delivery
2 P&G Plaza GO TE3 Cincinnati OH 45201

If related to South Boston On-Site Medical Plan: to the Band III Director Boston Site Medical Leader

OSMP Manager, South Boston Medical Plan, The Gillette Company, One Gillette Park, Mail Stop 1Y9 South Boston, MA 02127

This authorization shall expire upon the earlier occurrence of: (a) revocation of the authorization; (b) a finding by the Secretary of the U.S. Department of Health and Human Services that this authorization is not in compliance with requirements of HIPAA; (c) complete satisfaction of the purpose(s) for which this authorization was originally obtained, to be determined in the reasonable discretion of the Plan; or (d) six (6) years from the date this authorization is executed.

By signing this authorization you acknowledge and agree that any information used or disclosed pursuant to this authorization could be at risk for redisclosure by the recipient and no longer protected under HIPAA.

Please keep a copy of this signed authorization when you submit it to the Plan.

Acknowledged and agreed to by:

_____ _____
Your Name Date

[OR]

On behalf of _____
(*Participant or Beneficiary if you are authorized to agree for someone else such as your minor child*)

By: _____ _____
Your Name (as Representative of the person listed above) Date

As: _____
Capacity as Representative (how are you this person's authorized representative)

You should return this completed form to:

Band III Director, NA Health & Wellness, My P&G Services & US Benefits Delivery
2 P&G Plaza GO TE3 Cincinnati OH 45201

If related to South Boston On-Site Medical Plan: to the Band III Director Boston Site Medical Leader

OSMP Manager, South Boston Medical Plan, The Gillette Company, One Gillette Park, Mail Stop 1Y9 South Boston, MA 02127

This authorization is prepared pursuant to the requirements of the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191), 42 U.S.C. Section 1320d, *et seq.*, and regulations promulgated thereunder, as amended from time to time (collectively referred to as "HIPAA").

THE PROCTER & GAMBLE COMPANY

HIPAA PRIVACY

REQUEST FOR ACCESS TO DESIGNATED RECORDS

PARTICIPANT'S REQUEST

The Procter & Gamble Company and its subsidiaries (collectively, the "Company") sponsor certain self-insured group health plans in the United States (collectively, the "Plan").

Effective _____ [*date*], I, _____ [*please print full name*], am requesting access to that Protected Health Information ("PHI") contained in the Designated Record Set which the Plan or a Business Associate of the Plan maintains on my behalf and described as follows [*identify the information to be accessed and the requested time and manner of access as specifically as possible*] _____

_____

_____

_____

_____

_____

If you are requesting information regarding how the insurance company used or disclosed your information, you should contact your insurance carrier with the request. You will be required to complete a request form specific to that insurance carrier.

☐ Additional pages attached.

_____

Signature Date

[OR]

_____

Representative/Relationship Date

PLEASE DIRECT REQUESTS FOR ACCESS
OR QUESTIONS REGARDING THIS FORM TO:

Band III Director, NA Health & Wellness, My P&G Services & US Benefits Delivery
2 P&G Plaza GO TE3 Cincinnati OH 45201

If related to South Boston On-Site Medical Plan: to the Band III Director Boston Site Medical Leader

OSMP Manager, South Boston Medical Plan, The Gillette Company, One Gillette Park, Mail Stop 1Y9 South Boston, MA 02127

For Plan Use Only

Date Request Received: _____

Response Due Date: _____

Date Response (attached) sent: _____

THE PROCTER & GAMBLE COMPANY

HIPAA PRIVACY

RESPONSE TO REQUEST FOR ACCESS TO DESIGNATED RECORDS

PLAN'S RESPONSE

The Procter & Gamble Company and its subsidiaries (collectively, the "Company") sponsor certain self-insured group health plans in the United States (collectively, the "Plan").

On _____ [*date*], the Plan received the above-stated request for access to Protected Health Information ("PHI"). As of _____ [*date no later than thirty (30) days following date of receipt*], the Plan takes the following action with respect to your request:

☐ Grants all or part of your request. Specifically, the Plan will take the following requested action(s) _____.

☐ Denies all or part of your request. Specifically, the Plan will not take the following requested action(s) _____

_____

_____, based on the following reason(s):

☐ The information is not part of your designated record set.

☐ Under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), you are restricted from accessing this information because it falls within one of the following categories:

☐ psychotherapy notes;
☐ information compiled for civil, criminal, or administrative actions;
☐ it is subject to the Clinical Laboratory Improvements Amendments of 1988;
☐ regards inmates at correctional institutions;
☐ it was created during the course of research and, as you were previously advised, your rights to access the information have been temporarily suspended until _____[*date or event rights reinstated*];
☐ it is subject to the Federal Privacy Act (5 U.S.C. § 552(a)); or
☐ was not created by the Plan and was received under a seal of confidentiality
☐ allowed uses that do not need to be disclosed.

You have no right to contest a denial of access by the Plan if based on any of the above-stated reasons.

☐ Access is denied in the discretion of the Plan in the health and safety interests of the individual to which the information pertains or another third party. You have the right to

have this denial of access reviewed by a licensed healthcare professional designated by the Plan who did not participate in the original denial of your request by submitting a written statement to the Plan requesting a review of the denial. You also have the right to file a complaint about your denial to us or to the Office of Civil Rights, U. S. Department of Health and Human Services. Please contact the Plan's Privacy Official at _____
_____

to learn about the applicable complaint procedures.

☐ other_____
_____

☐ additional pages attached.

☐ The Plan does not maintain the protected health information that is the subject of your request. The information is maintained by, and you should direct your request for access to: _____
_____

☐ Requests a thirty (30) day extension of time within which to respond to your request for the following reason(s) _____
_____
_____. The Plan will act on your request by _____[*date no later than sixty (60) days following date of receipt*].

_____
[PLAN]

By: _____
Its: _____
Date: _____

A COPY OF THIS DOCUMENT SHALL BE PROVIDED TO THE PARTICIPANT OR BENEFICIARY TO WHOM THE INFORMATION IN THIS REQUEST PERTAINS.

Please direct questions regarding this form or the applicable complaint procedures to:

Band III Director, NA Health & Wellness, My P&G Services & US Benefits Delivery

2 P&G Plaza GO TE3 Cincinnati OH 45201

If related to South Boston On-Site Medical Plan: to the Band III Director Boston Site Medical Leader

OSMP Manager, South Boston Medical Plan, The Gillette Company, One Gillette Park, Mail Stop 1Y9 South Boston, MA 02127

THE PROCTER & GAMBLE COMPANY

HIPAA PRIVACY

REQUEST FOR AMENDMENT OF DESIGNATED RECORDS

REQUEST

The Procter & Gamble Company and its subsidiaries (collectively, the "Company") sponsor certain self-insured group health plans in the United States (collectively, the "Plan").

Effective _____[*date*], I, _____ *[please print full name*], am requesting that the Protected Health Information ("PHI") contained in the Designated Record Set which the Plan or a Business Associate of the Plan maintains on my behalf be amended as follows: [*identify the information to be amended and the requested amendment as specifically as possible*]_____
_____
_____
_____
_____

☐ Additional pages attached.

_____
Signature Date

[OR]

_____
Representative/Relationship Date

PLEASE DIRECT REQUESTS FOR AMENDMENTS
OR QUESTIONS REGARDING THIS FORM TO:

Band III Director, NA Health & Wellness, My P&G Services & US Benefits Delivery
2 P&G Plaza GO TE3 Cincinnati OH 45201

If related to South Boston On-Site Medical Plan: to the Band III Director Boston Site Medical Leader

OSMP Manager, South Boston Medical Plan, The Gillette Company, One Gillette Park, Mail Stop 1Y9 South Boston, MA 02127

For Plan Use Only

Date Request Received: _____

Response Due Date: _____

Date Response (attached) sent: _____

THE PROCTER & GAMBLE COMPANY

HIPAA PRIVACY RESPONSE TO REQUEST FOR

AMENDMENT OF DESIGNATED RECORDS

PLAN'S RESPONSE

The Procter & Gamble Company and its subsidiaries (collectively, the "Company") sponsor certain self-insured group health plans in the United States (collectively, the "Plan").

On _____ [*date*], the Plan received the above-stated request for amendment of Protected Health Information ("PHI"). As of _____ [*date no later than sixty (60) days following date of receipt*], the Plan takes the following action with respect to your request:

☐ Grants all or part of your request. Specifically, the Plan will take the following requested action(s) _____
_____
_____.

Please notify the Plan in writing of all persons or entities, and their addresses, to which you would like notification of this change to be sent _____
_____
_____
_____.

☐ Denies all or part of your request. Specifically, the Plan will not take the following requested action(s) _____
_____,

based on the following reasons:

☐ The information was not created by the Plan;
☐ The information is not part of your Designated Record Set;
☐ The information is accurate and complete;
☐ Under HIPAA, you are restricted from accessing or amending this information;
or
☐ Other _____
_____.
☐ Additional pages attached.

You have the right to contest this denial of amendment by the Plan by submitting a written statement of disagreement to the Privacy Official of the Plan at the address below. Even if you do not submit a statement of disagreement, you may request in writing to the Privacy Official at the address below that the Plan include your written request for amendment and the Plan's denial thereof with any future disclosures of that information. You also have the right to file a complaint about your denial to the Plan or to the Office of Civil Rights, U. S.

Department of Health and Human Services. **Please contact the Plan's Privacy Official at pgprivacyofficer.im@pg.com to learn about the applicable complaint procedures.**

☐ Requests a thirty (30) day extension of time within which to respond to your request for the following reason(s)_____

_____

_____

The Plan will act on your request by _____ [*date no later than ninety (90) days following date of receipt*].

[Plan]

By: _____

Its: _____

Date: _____

THE PROCTER & GAMBLE COMPANY

HIPAA PRIVACY REBUTTAL TO

AMENDMENT OF DESIGNATED RECORD SET

PLAN'S REBUTTAL

The Procter & Gamble Company and its subsidiaries (collectively, the "Company") sponsor certain self-insured group health plans in the United States (collectively, the "Plan").

On _____ [*date statement of disagreement was received*], _____ [*name of participant or beneficiary*] filed a statement of disagreement to the Plan's denial of his/her request for amendment dated _____. The Plan responds to this statement of disagreement as follows:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

☐ Additional pages attached.

COPIES OF THIS DOCUMENT SHALL BE APPENDED TO THE INFORMATION TO WHICH IT PERTAINS IN A DESIGNATED RECORD SET AND WILL BE PROVIDED WITH ANY FUTURE DISCLOSURES OF SUCH INFORMATION UPON THE PARTICIPANT'S OR BENEFICIARY'S REQUEST.

Please direct questions regarding this form and the Plan's complaint procedures to:

Band III Directorr, NA Health & Wellness, My P&G Services & US Benefits Delivery
2 P&G Plaza GO TE3 Cincinnati OH 45201

If related to South Boston On-Site Medical Plan: to the Band III Director Boston Site Medical Leader

OSMP Manager, South Boston Medical Plan, The Gillette Company, One Gillette Park, Mail Stop 1Y9 South Boston, MA 02127

THE PROCTER & GAMBLE COMPANY

HIPAA PRIVACY REQUEST FOR

ACCOUNTING OF DISCLOSURES OF

PROTECTED HEALTH INFORMATION

REQUEST

The Procter & Gamble Company and its subsidiaries (collectively, the "Company") sponsor certain self-insured group health plans in the United States (collectively, the "Plan").

Effective _____ [*date*], I, _____ [*please print full name*], am requesting an accounting of all disclosures of my Protected Health Information ("PHI") by the Plan, or any of its Business Associates, for the period beginning _____ and ending on _____ [*up to a maximum of six (6) years prior to the date of this request (three (3) years for requests of electronic health records related to treatment, payment, or healthcare operations)*].

Specifically, I would like to limit this request for accounting to include disclosures only pertaining to the following [*identify the accounting or specific event or treatment as specifically as possible*]

_____

_____

_____

_____

_____

_____

Signature Date

[OR]

_____

Representative/Relationship Date

_____

PLEASE DIRECT REQUESTS FOR ACCOUNTINGS
OR QUESTIONS REGARDING THIS FORM TO:

Band III Director, NA Health & Wellness, My P&G Services & US Benefits Delivery
2 P&G Plaza GO TE3 Cincinnati OH 45201

If related to South Boston On-Site Medical Plan: to the Band III Director Boston Site Medical Leader

OSMP Manager, South Boston Medical Plan, The Gillette Company, One Gillette Park, Mail Stop 1Y9 South Boston, MA 02127

For Plan Use Only

Date Request Received: _____
Response Due Date: _____
Date Response (attached) sent: _____

THE PROCTER & GAMBLE COMPANY

HIPAA PRIVACY

RESPONSE TO REQUEST FOR

ACCOUNTING OF DISCLOSURES OF

PROTECTED HEALTH INFORMATION

PLAN'S RESPONSE

The Procter & Gamble Company and its subsidiaries (collectively, the "Company") sponsor certain self-insured group health plans in the United States (collectively, the "Plan").

On _____ [*date*], the Plan received the above-stated request for an accounting. As of today, _____ [*date no later than sixty (60) days following date of receipt of the request*], the Plan takes the following action with respect to your request:

☐ Grants your request. Please see the enclosed accounting that contains for each disclosure: the date of the disclosure, the name of the entity or person who received the disclosure (and if known, his/her/its address); a brief description of the Protected Health Information ("PHI") disclosed; and a brief statement of the purpose of the disclosure and the basis for the disclosure.

☐ Denies your request. You do not have a right to an individual accounting and we have no relevant records because any disclosure of your PHI was due to any one or more of the following reasons:

For treatment;

For payment;

For healthcare operations;

To you;

Pursuant to your authorization;

For notification purposes;

For national security purposes;

To a correctional institution or for law enforcement purposes;

As part of a Limited Data Set;

Occurred more than six (6) years prior to the date on which the accounting was requested; or

Was incident to an otherwise permitted use or disclosure.

☐ Requests a thirty (30) day extension of time within which to respond to your request for the following reason(s) _____
_____.
The Plan will act on your request by _____ [*date no later than ninety (90) days following date of receipt*].

[Plan]

By: _____
Its: _____
Date: _____

PLAN'S RESPONSE

☐ No charge, first accounting this twelve (12) month period.

☐ *$_____ [reasonable cost-based fee for additional accountings within one twelve (12) month period].*

Please direct questions regarding this form or the Plan's complaint procedure to:

Band III Director, NA Health & Wellness, My P&G Services & US Benefits Delivery
2 P&G Plaza GO TE3 Cincinnati OH 45201

If related to South Boston On-Site Medical Plan: to the Band III Director Boston Site Medical Leader

OSMP Manager, South Boston Medical Plan, The Gillette Company, One Gillette Park, Mail Stop 1Y9 South Boston, MA 02127

THE PROCTER & GAMBLE COMPANY

REQUEST FOR RESTRICTIONS ON USE &

DISCLOSURE/CONFIDENTIAL COMMUNICATIONS FORM

Name of Individual: _____

Date: _____

I am requesting that use and access to my Protected Health Information ("PHI") be restricted in the following manner:

_____

_____

_____

_____

_____

_____

_____

_____

Disclosure of all or part of the information to which this request pertains could endanger me. Therefore, I am requesting that communication involving PHI be provided to me in the following manner or at the following alternative address:

_____

_____

_____

_____

_____

Signature of Individual Requesting Restriction: _____

Signature of Personal Representative acting on behalf of the Individual, if the Individual is not making the Request for Restriction: _____

PLEASE DIRECT REQUESTS FOR RESTRICTIONS ON USE
AND DISCLOSURE/CONFIDENTIAL COMMUNICATIONS
OR QUESTIONS REGARDING THIS FORM TO:

Band III Director, NA Health & Wellness, My P&G Services & US Benefits Delivery
2 P&G Plaza GO TE3 Cincinnati OH 45201

If related to South Boston On-Site Medical Plan: to the Band III Director Boston Site Medical Leader

OSMP Manager, South Boston Medical Plan, The Gillette Company, One Gillette Park, Mail Stop 1Y9 South Boston, MA 02127

THE PROCTER & GAMBLE COMPANY

RESPONSE FOR RESTRICTIONS ON USE &

DISCLOSURE/CONFIDENTIAL COMMUNICATIONS FORM

Date: _____

Date of Request for Privacy Protection: _____

Name of Individual Requesting Privacy Protection: _____

Your Request for Privacy Protection has been denied/accepted :_____

Your Request was denied for the following reasons:

_____

_____

_____

_____

Name of Privacy Official: _____

Signature of Privacy Official: _____

ATTENTION

IF THE REQUEST PERTAINS TO CONFIDENTIAL COMMUNICATIONS, VERIFY THAT THIS RESPONSE COMPLIES WITH THE REQUEST, IF THE REQUEST IS ACCEPTED

_____

THE PROCTER & GAMBLE COMPANY

REQUEST FOR ACCESS TO PROTECTED HEALTH INFORMATION

WITHOUT AUTHORIZATION FROM INDIVIDUAL

Name of Individual for whom Protected Health

Information ("PHI") is requested: _____

Name of Party Requesting: _____

Address: _____

Address: _____

I am requesting that I be allowed to inspect and copy the following PHI:

_____

_____

_____

Reason for Request for PHI: _____

_____

Signature of Individual Requesting Access to PHI: _____

Date of Request: _____

Attach copy of Individual's identification to this form along with all other documentation of the reason for disclosure (e.g., subpoena, court order, etc.).

PLEASE DIRECT REQUESTS FOR DISCLOSURES OR QUESTIONS
REGARDING THIS FORM TO:

Band III Director, NA Health & Wellness, My P&G Services & US Benefits Delivery
2 P&G Plaza GO TE3 Cincinnati OH 45201

If related to South Boston On-Site Medical Plan: to the Band III Director Boston Site Medical Leader

OSMP Manager, South Boston Medical Plan, The Gillette Company, One Gillette Park, Mail Stop 1Y9 South Boston, MA 02127

THE PROCTER & GAMBLE COMPANY

HIPAA PRIVACY

COMPLAINT FORM

The Procter & Gamble Company and its subsidiaries (collectively, the "Company") sponsor certain self-insured group health plans in the United States (collectively, the "Plan"). This is a complaint regarding the actions, policies and procedures, or Notice of Privacy Practices of the Plan and/or regarding actions of the Plan with respect to the individually identifiable health information of _____ [*Name of Participant or Beneficiary*]. Filing this Complaint Form will not affect the benefits you receive from the Plan, nor will the Plan retaliate or discriminate against you in any manner in response to your complaint.

Please complete the following form, sign and date it, and return it to Privacy Official, _____ _____ If you have any questions or concerns regarding this form or where to send it, please contact the Privacy Official at the aforementioned address. You may also file a copy of this complaint in writing with the U. S. Department of Health and Human Services, Office of Civil Rights, or via e-mail using the information at. For filing information for the Office of Civil Rights please contact the Plan at the number, address, or e-mail listed above.

Complainant:

Name_____

Address_____

Telephone: _____ E-mail address: _____

SSN#: _____

Complaint

Please provide a short description of your complaint and how you would like the Plan to address or resolve your complaint:_____

_____

_____

_____

_____

_____

☐ additional pages attached.

I certify that the statements made in this complaint are true and correct to the best of my knowledge and belief.

Signature	Date	Representative/Relationship	Date

OR

PLEASE DIRECT COMPLAINTS OR QUESTIONS REGARDING THIS FORM TO:

Band III Director, NA Health & Wellness, My P&G Services & US Benefits Delivery
2 P&G Plaza GO TE3 Cincinnati OH 45201

If related to South Boston On-Site Medical Plan: to the Band III Director Boston Site Medical Leader

OSMP Manager, South Boston Medical Plan, The Gillette Company, One Gillette Park, Mail Stop 1Y9 South Boston, MA 02127

COMPLAINING PARTY: PLEASE RETAIN A COPY FOR YOUR RECORDS

THE PROCTER & GAMBLE COMPANY

REPORT OF COMPLAINT INVESTIGATION FORM

Current Date: _____

Date of Incident: _____

Name of Complaining Party: _____

Name of Individual(s) perceived to have violated the privacy policies and procedures:

_____

Report of investigation of complaint regarding violation of privacy policies and procedures:

_____

_____

_____

_____

_____

_____

_____

_____

Corrective measures, if any, and date of implementation: _____

_____

Name of Privacy Official: _____

Signature of Privacy Official: _____

APPENDIX C NOTICES OF PRIVACY PRACTICES

EFFECTIVE DATE: 6/1/2022

SOUTH BOSTON ON-SITE MEDICAL PLAN

HIPAA NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

This Notice of Privacy Practices ("Notice") describes the legal obligations of the South Boston On-Site Medical Plan ("OSMP" or "Plan") and your legal rights regarding your protected health information held by the Plan under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Among other things, this Notice describes how your protected health information may be used and disclosed to carry out treatment, payment, or health care operations, or for any other purposes that are permitted or required by law. HIPAA requires the Plan to provide this Notice to you.

The HIPAA Privacy Rule protects certain medical information known as "protected health information." Under HIPAA, protected health information is individually identifiable health information, including demographic information, collected from you or created or received by a health care provider, a health care clearinghouse, a health plan, or your employer in its role as a sponsor of a group health plan, that relates to (1) your past, present, or future physical or mental health or condition; (2) the provision of health care to you; or (3) the past, present, or future payment for the provision of health care to you. For purposes of this Notice, we will refer to your protected health information as either "medical information about you" or "your medical information."

If you have any questions about this Notice or about the Plan's privacy practices, please contact the OSMP Manager.

Our Pledge Regarding Medical Information

We understand that medical information about you and your health is personal. Protecting medical information about you is important to us. This Notice applies to all of the records of your care generated and maintained by OSMP containing your medical information, whether made by health care professionals or other personnel.[1]

We are required under HIPAA to:

- maintain the privacy of medical information about you;

[1] Note that the services provided under the OSMP are provided at the same location as the *Vibrant Living Health Center* at the South Boston World Shaving Headquarters. The services provided by the *Vibrant Living Health Center* (e.g., first aid, occupational screenings, emergency care) are not covered by this Notice. This Notice pertains to primary and preventative care services you receive under the OSMP. However, The Procter and Gamble Company also takes care to protect the confidentiality of your information that is used/received by the *Vibrant Living Health Center* outside of the OSMP. For more information about the *Vibrant Living Health Center's* maintenance of your private information, please refer to the Company's Employee Privacy Policy.

- give you this Notice of our legal duties and privacy practices with respect to medical information about you;
- notify you following a breach of unsecured medical information about you, and
- follow the terms of the notice that is currently in effect.

This Notice is a summary of our duties and your rights under the HIPAA Privacy Rule. If a state enacts legislation or imposes standards that provide you with additional rights or protections, we will comply with the additional state requirements. If you have any questions, please contact the OSMP Manager.

Who Will Follow This Notice

All employees, staff and other personnel who may need access to your medical information follow the terms of this Notice.

How We May Use and Disclose Medical Information About You

Under HIPAA, the Plan may use or disclose your medical information under certain circumstances without your permission. We (including third-party administrators) may use and disclose your medical information for treatment, payment and health care operations, as described below.

For Treatment. The Plan may use or disclose medical information about you to facilitate medical treatment or services by health care providers, including doctors, nurses, technicians, training doctors, or other health care professionals who are involved in taking care of you. For example, the Plan might disclose information about your health to another of your health care providers.

For Payment. The Plan may use or disclose medical information about you to determine your eligibility for Plan benefits, to facilitate payment for the treatment and services you receive from health care providers, to determine benefit responsibility under the Plan, or to coordinate Plan coverage. For example, the Plan may inform your health care provider about your medical history to determine whether a particular treatment is experimental, investigational, or medically necessary, or to determine whether the Plan will cover the treatment. The Plan may also share medical information about you with a utilization review or precertification service provider. Likewise, the Plan may share medical information about you with another entity to assist with the adjudication or subrogation of health claims or to another health plan to coordinate benefit payments.

For Health care Operations. The Plan may use and disclose medical information about you for other Plan operations that are necessary to run the Plan. For example, the Plan may use your medical information in connection with conducting quality assessment and improvement activities; underwriting (subject to certain limitations as described below), 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.

We are also allowed or required to share your medical information, without your authorization, in certain situations or when certain conditions have been met, as described below. ***Health-Related Benefits and Services.*** We may use and disclose medical information about you to tell you about health-related benefits or services under the Plan that may be of interest to you.

As Required By Law. The Plan may disclose medical information about you when required to do so by federal, state or local law. For example, the Plan may disclose your medical information when required by national security laws or public health disclosure laws.

HHS. The Plan may be required to disclose medical information about you to the Secretary of the Department of Health and Human Services if the Secretary is investigating or determining whether the Plan has complied with the HIPAA Privacy Rule.

To Avert a Serious Threat to Health or Safety. The Plan may use and disclose medical information about you to help with public health and safety issues when we are required or permitted to do so, including to prevent a serious threat to your health and safety or the health and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat. For example, the Plan may disclose your medical information in a proceeding regarding the licensure of a physician.

To Plan Sponsors. For purposes of administering the Plan, the Plan may disclose medical information about you to certain employees of the Company. However, those employees will only use or disclose that information as necessary to perform plan administration functions or as otherwise required by HIPAA, unless you have authorized further disclosures. Your medical information cannot be used for employment purposes without your specific authorization.

To Business Associates. We may enter into contracts with individuals and entities known as Business Associates that perform services for us. Our Business Associates may need access to your medical information to perform these services. Our Business Associates are required by law and their agreements with us to appropriately safeguard the medical information they receive in connection with providing their services.

Special Situations

In addition to the above, the following categories describe other possible ways that the Plan may use and disclose your medical information without your authorization.

Organ and Tissue Donation. If you are an organ donor, the Plan may release medical information about you to organizations that handle organ procurement or organ, eye, or tissue transplantation, or to an organ bank, as necessary to facilitate organ or tissue donation or transplantation.

Military and Veterans. If you are a member of the armed forces, the Plan may release medical information about you as required by military command authorities. The Plan may also release medical information about you to foreign military authorities if you are a member of that foreign military.

Correctional Institutions. If you become an inmate of a correctional institution, the Plan may release medical information about you to such institution, when necessary for your health or the health and safety of others.

Workers' Compensation. The Plan may release medical information about you for workers' compensation or similar programs. These programs provide benefits for work-related injuries or illness.

Public Health Risks. The Plan may disclose medical information about you for public health activities. These activities generally include the following:

- to prevent or control disease, injury or disability;
- to report births and deaths;
- to report child abuse or neglect;
- to report reactions to medications or problems with products;
- to notify people of recalls of products they may be using;
- to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition; and
- to notify the appropriate government authority if the Plan believes a patient has been the victim of abuse, neglect or domestic violence. The Plan will only make this disclosure if you agree, or when required or authorized by law.

Health Oversight Activities. The Plan may disclose medical information about you to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

Lawsuits and Disputes. The Plan may disclose medical information about you in response to a court order, administrative order, subpoena, discovery request, or other lawful procedure, if you are involved in the lawsuit or dispute. The Plan will only disclose your medical information if efforts have been made to inform you about the request or to obtain a protective order with respect to your medical information.

Law Enforcement. The Plan may disclose medical information about you if asked to do so by a law enforcement official (1) in response to a court order, subpoena, warrant, summons, or similar process; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) about the victim of a crime, if under certain limited circumstances, you are the victim and the Plan is unable to obtain the your agreement; (4) about a death that the Plan believes may be the result of criminal conduct; or (5) about criminal conduct.

Coroners, Medical Examiners, and Funeral Directors. The Plan may release medical information about you to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. The Plan may also release medical information about you to a funeral director, as necessary to carry out the director's duties.

National Security and Intelligence Activities. The Plan may release medical information about you to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

Research. The Plan may disclose medical information about you to researchers, when individual identifiers have been removed or when an institutional review board or privacy board has reviewed the research proposal and established protocols to ensure the privacy of the requested information, and approves the research.

Personal Representatives. The Plan will disclose medical information about you to individuals you have authorized or individuals designated as your personal representative, attorney-in-fact, etc., so long as you provide the Plan with a written authorization and any supporting documents (such as a power of attorney). However, the Plan is not required to disclose information to a personal representative if the Plan reasonably believes that (1) you have been or may be subject to domestic violence, abuse, or neglect by such person, or (2) treating such person as your personal representative could endanger you, or (3) in the exercise of professional judgment, the Plan decides that it is in your best interests not to treat such person as your personal representative.

Spouses and Other Family Members. The Plan will send all mail related to all covered individuals to an employee, except for limited circumstances. However, if a covered individual requests restrictions or confidential communications (see below) and the Plan has agreed to such request, the Plan will send mail in accordance with such request.

Underwriting. We may use or disclose medical information about you for underwriting purposes, but we are prohibited from using or disclosing any genetic information about you for such purposes.

Authorizations

Other uses and disclosures of your medical information not covered by this Notice or the laws that apply to the Plan will be made only with your written authorization. If you provide the Plan with written authorization to use or disclose medical information about you (for a purpose that requires that authorization), you may revoke that authorization, in writing, at any time. If you revoke your authorization, thereafter the Plan will no longer use or disclose medical information about you for the reasons covered by your written authorization. However, the revocation is only effective with regard to future uses and disclosures. The Plan is unable to undo any uses or disclosures that were made before such revocation.

The Plan will not use or disclose medical information about you without a written authorization from you in the following specific situations:

Psychotherapy Notes. The Plan will not use or disclose psychotherapy notes about you without a written authorization, unless (a) the disclosure is to the originator of the notes for treatment purposes, (b) the use or disclosure is to defend the Plan in a legal action or proceeding brought by you, (c) the use or disclosure is required by the Secretary of the Department of Health and Human Services, or (d) the use or disclosure is permitted because the disclosure is (i) required by law, (ii) to a health oversight agency for oversight activities authorized by law related to the originator of the notes, (iii) to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause

of death, or other duties as authorized by law, or (iv) to prevent or lessen a serious or imminent threat to the health or safety of a person or the public, where such disclosure is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.

Marketing. The Plan will not use or disclose medical information about you for marketing purposes without a written authorization, unless the communication is (a) a face-to-face communication by the Plan to you, or (b) a promotional gift of nominal value from the Plan to you. Further, the Plan will not receive financial remuneration from a third party with respect to any marketing unless your authorization states that remuneration is involved.

Sale. The Plan will not sell medical information about you without a written authorization that includes a statement that such disclosure will result in remuneration to the Plan.

Your Rights Regarding Medical Information About You

You have the following rights regarding medical information about you:

Right to Access. You have the right to inspect and obtain a copy of medical information that we maintain about you in certain records maintained by the Plan. The Plan is required to disclose to you medical information contained in your medical records; billing records; enrollment, payment, claims adjudication, and case or medical management record systems; and any other records used to make decisions regarding your health care benefits.

To inspect and obtain a copy of your medical information, you must submit a written request to the Plan's third-party administrator or your insurance carrier listed in the Summary Plan Descriptions or Summary of Material Modifications. If you request a copy of your medical information, a reasonable fee may be charged for the costs of copying, mailing or other supplies associated with your request.

Your request to inspect and copy may be denied in certain very limited circumstances. If you are denied access to your medical information, you may request that the denial be reviewed by submitting a request to the P&G Policy Committee.

P&G Policy Committee
c/o Assistant Secretary
Corporate Secretary's Office
P&G Plaza, C9-159
Cincinnati, OH 45202

Right to Amend. If you believe that the Plan's medical information about you is incorrect or incomplete, you may ask to amend the information. You have the right to request an amendment for as long as the information is kept by or for the Plan.

To request an amendment, your request must be made in writing and submitted to the third-party administrator or your insurance carrier listed in the Summary Plan Descriptions or Summary of Material Modifications. In addition, you must provide a reason that supports your request.

Your request for an amendment may be denied if it is not in writing or does not include a reason to support the request. In addition, your request may be denied if you ask to amend medical information that:

- was not created by the Plan, unless you provide a reasonable basis to believe that the person or entity that created the information is no longer available to make the amendment;
- is not part of the medical information kept by the Plan;
- is not part of the medical information which you would be permitted to inspect and copy; or
- is already accurate and complete.

If the Plan denies your request, you have the right to file a statement of disagreement with the Plan's decision, and we may give a rebuttal to your statement.

Right to an Accounting of Disclosures. For most disclosures of your medical information other than those specified below, you have the right to request an accounting of the disclosures we made in the six years prior to the date of your request. An accounting of disclosures will not include (1) disclosures made for purposes of treatment, payment, or health care operations; (2) disclosures made directly to you; (3) disclosures made pursuant to your written authorization; (4) disclosures made to friends or family involved in your care, in your presence or because of an emergency; (5) disclosures for national security purposes; or (6) disclosures incidental to otherwise permissible disclosures. The right to receive an accounting of disclosures of your medical information is subject to certain other exceptions, restrictions, and limitations.

To request an accounting of disclosures, you must submit your request in writing to the third-party administrator or your insurance carrier listed in the Summary Plan Descriptions or Summary of Material Modifications. Your request must state a time period that may not be longer than six years prior to the date of your request. The first accounting you request within a 12-month period will be provided free of charge, but you will be charged for the cost of providing additional accountings within that time period. You will be notified of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

Right to Request Restrictions on Certain Uses and Disclosures. You have the right to request that the Plan restrict certain uses and disclosures of your medical information for treatment, payment, or health care operations. You also have the right to request that the Plan limit the medical information about you that the Plan discloses to someone who is involved in your care or the payment for your care, like a family member or friend.

Except as provided in the next paragraph, the Plan is not required to agree to your request. If the Plan agrees to your request, the Plan will comply with your request until you revoke it or we notify you that we no longer agree to such restriction or limitation.

The Plan will comply with a restriction request if the disclosure of your medical information is (1) to another health plan and is for the purpose of carrying out payment or health care operations (but not treatment), (2) not otherwise required by law, and (3) pertains

solely to a health care item or service for which you, or a person on your behalf, has paid out-of-pocket in full.

To request such restrictions, you must make your request in writing to the third-party administrator or your insurance carrier listed in the Summary Plan Descriptions or Summary of Material Modifications. In your request, you must state (1) what information you want to limit; (2) whether you want to limit the Plan's use, disclosure, or both; and (3) to whom you want the limits to apply (for example, disclosures to your spouse).

Right to Request Confidential Communications. You have the right to request that the Plan communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that the Plan only contact you at work or by mail.

To request confidential communications, you must make your request in writing to the third-party administrator or your insurance carrier listed in the Summary Plan Descriptions or Summary of Material Modifications. The Plan will not ask you for the reason for your request. Your request must specify how or where you wish to be contacted. The Plan will accommodate all reasonable requests if you clearly provide information that the disclosure of all or part of your medical information could endanger you.

Right to a Paper Copy of This Notice. You have the right to receive a paper copy of this Notice at any time, even if you have previously agreed to receive this Notice electronically. To obtain a paper copy of this Notice, please request one in writing from the OSMP Manager.

Changes to this Notice

The Plan reserves the right to change this Notice. The Plan reserves the right to make the revised or changed Notice effective for medical information that the Plan already has about you as well as any medical information about you the Plan receives in the future. The Plan will post a copy of the current Notice on our website, at https://pgone.sharepoint.com/sites/boston/pages/default.aspx https://www5.lifeatworkportal.com/portal60/home#/portal/view/HOME

The effective date of the Notice will be listed on the first page of the Notice.

Complaints

If you have questions or would like additional information about our privacy practices, you may contact the Plan's Privacy Official by sending an email to corporateprivacy.im@pg.com. If you believe your privacy rights have been violated, you may file a complaint with the Plan or with the Secretary of the United States Department of Health and Human Services. To file a complaint with the Plan, contact the Healthcare Benefits Manager, at:

Healthcare Benefits Manager
South Boston Medical Plan
c/o U.S. Healthcare Benefits
The Procter & Gamble Company
2 P&G Plaza, TE-3, Box 4A

Cincinnati, OH 45202

If you are an active employee, you also may file a complaint with the Plan's Privacy Official by sending an email to pgprivacyofficer.im@pg.com. All complaints must be submitted in writing. You will not be penalized, or in any other way retaliated against, for filing a complaint with the Plan or the Secretary of the United States Department of Health and Human Services.

Privacy Official

The Global Privacy Officer of The Procter & Gamble Company is the Privacy Official for the Plan. Please check www.pg.com/privacy for more information.

Contact Information

OSMP Manager
South Boston Medical Plan
The Gillette Company
One Gillette Park, Mail Stop 1Y9
South Boston, MA 02127
Phone: 617-463-2222
Fax: 617-463-4122

Healthcare Benefits Manager
South Boston Medical Plan
c/o U.S. Healthcare Benefits
The Procter & Gamble Company
2 P&G Plaza, TE-3, Box 4A
Cincinnati, OH 45202

ACKNOWLEDGMENT OF RECEIPT OF PRIVACY NOTICE

I, _____, hereby acknowledge that, on the date written below, I received a copy of the South Boston On-Site Medical Plan's HIPAA Notice of Privacy Practices.

_____ _____

Signature of Participant (or Authorized Representative) Date

_____

Name (Please Print)

_____

Relationship to Participant (if Authorized Representative)

HIPAA NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSEDAND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

This Notice of Privacy Practices ("Notice") describes the legal obligations of all group health plans (with the exception of the South Boston On-Site Medical Plan, which maintains its own Notice) in the United States sponsored, administered, and self-insured by The Procter & Gamble Company and its affiliates (collectively the "Plan"), and your legal rights regarding your protected health information held by the Plan under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Among other things, this Notice describes how your protected health information may be used and disclosed to carry out treatment, payment, or health care operations, or for any other purposes that are permitted or required by law. HIPAA requires the Plan to provide this Notice to you.

The HIPAA Privacy Rule protects certain medical information known as "protected health information." Under HIPAA, protected health information is individually identifiable health information, including demographic information, collected from you or created or received by a health care provider,a health care clearinghouse, a health plan, or your employer in its role as a sponsor of a group health plan, that relates to (1) your past, present, or future physical or mental health or condition; (2) the provision of health care to you; or (3) the past, present, or future payment for the provision of health care to you. For purposes of this Notice, we will refer to your protected health information as either "medicalinformation about you" or "your medical information."

If you have any questions about this Notice or about the Plan's privacy practices, please contact the Plan's Privacy Official at corporateprivacy.im@pg.com or the Director, U.S. Health and Wellness Benefits, GBS-My P&G Services (or equivalent).

Effective Date: This Notice is effective October 1, 2022.

• Our Pledge Regarding Medical Information

We understand that medical information about you and your health is personal. Protecting medical information about you is important to us. This Notice applies to all of the records of your care generated and maintained by the Plan containing your medical information, whether made by health care professionals or other personnel.

We are required under HIPAA to:

- maintain the privacy of medical information about you;
- give you this Notice of our legal duties and privacy practices with respect to medical information about you;
- notify you following a breach of unsecured medical information about you; and
- follow the terms of the notice that is currently in effect.

This Notice is a summary of our duties and your rights under the HIPAA Privacy Rule. If a state enacts legislation or imposes standards that provide you with additional rights or protections, we will comply with the additional state requirements. If you have any questions, please contact the Plan's Privacy Official at corporateprivacy.im@pg.com or the Director, U.S. Health and Wellness Benefits, GBS-My P&G Services (or equivalent).

- ## Who Will Follow This Notice

All employees, staff and other personnel who may need access to your medical information will follow the terms of this Notice.

- ## How We May Use and Disclose Medical Information About You

Under HIPAA, the Plan may use or disclose your medical information under certain circumstances without your permission. We (including third-party administrators) may use and disclose your medical information for treatment, payment, and health care operations, as described below.

- **For Treatment.** The Plan may use or disclose medical information about you to facilitate medical treatment or services by health care providers, including doctors, nurses, technicians, training doctors, orother health care professionals who are involved in your medical care. For example, the Plan might disclose information about your prior prescriptions to a pharmacist to determine if prior prescriptions contradict a pending prescription.
- **For Payment.** The Plan may use or disclose medical information about you to determine your eligibility for Plan benefits, to facilitate payment for the treatment and services you receive from health care providers, to determine benefit responsibility under the Plan, or to coordinate Plan coverage. For example, the Plan may inform your health care provider about your medical history to determine whether a particular treatment is experimental, investigational, or medically necessary, or to determine whether the Plan will cover the treatment. The Plan may also share medical information about you witha utilization review or pre-authorization service provider. Likewise, the Plan may share medical information about you with another entity to assist with the adjudication or subrogation of health claims or to another health plan to coordinate benefit payments.
- **For Health Care Operations.** The Plan may use and disclose medical information about you for other Plan operations that are necessary to run the Plan. For example, the Plan may use your medical information in connection with conducting quality assessment and improvement activities; underwriting (subject to certain limitations as described below), 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.

We are also allowed or required to share your medical information, without your authorization, in certain situations or when certain conditions have been met, as described below.

- **Health-Related Benefits and Services.** We may use and disclose medical information about you to tell you about health-related benefits or services under the Plan that may be of interest to you.
- **As Required By Law.** The Plan may disclose medical information about you when required to do so by federal, state, or local law. For example, the Plan may disclose your medical information when required by national security laws or public health disclosure laws.
- **HHS.** The Plan may be required to disclose medical information about you to the Secretary of the Departmentof Health and Human Services if the Secretary is investigating or determining whether the Plan has complied with the HIPAA Privacy Rule.

- **To Avert a Serious Threat to Health or Safety.** The Plan may use and disclose medical information about you to help with public health and safety issues when we are required or permitted to do so, including to prevent a serious threat to your health and safety or the health and safetyof the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat. For example, the Plan may disclose your medical information in a proceeding regarding the licensure of a physician.
- **To Plan Sponsors.** For purposes of administering the Plan, the Plan may disclose medical informationabout you to certain employees of the Company. However, those employees will only use or disclose that information as necessary to perform plan administration functions or as otherwise required by HIPAA, unless you have authorized further disclosures. Your medical information cannot be used for employment purposes without your specific authorization.
- **To Business Associates.** We may enter into contracts with individuals and entities known as Business Associates that perform services for us. Our Business Associates may need access to your medical information to perform these services. Our Business Associates are required by law and their agreements with us to appropriately safeguard the medical information they receive in connection with providing their services.

• Special Situations

In addition to the above, the following categories describe other possible ways that the Plan may use and disclose your medical information without your authorization.

- **Organ and Tissue Donation.** If you are an organ donor, the Plan may release medical information aboutyou to organizations that handle organ procurement or organ, eye, or tissue transplantation, or to an organ bank, as necessary to facilitate organ or tissue donation or transplantation.
- **Military and Veterans.** If you are a member of the armed forces, the Plan may release medical information about you as required by military command authorities. The Plan may also release medicalinformation about you to foreign military authorities if you are a member of that foreign military.
- **Correctional Institutions.** If you become an inmate of a correctional institution, the Plan may release medical information about you to such institution, when necessary for your health or the health and safety of others.
- **Workers' Compensation.** The Plan may release medical information about you for workers' compensation or similar programs. These programs provide benefits for work-related injuries or illness.
- **Public Health Risks.** The Plan may disclose medical information about you for public health activities.These activities generally include the following:
  - to prevent or control disease, injury, or disability;
  - to report births and deaths;
  - to report child abuse or neglect;
  - to report reactions to medications or problems with products;
  - to notify people of recalls of products they may be using;
  - to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition; and

  - to notify the appropriate government authority if the Plan believes a patient has been the victim of abuse, neglect, or domestic violence. The Plan will only make this disclosure if you agree or when required or authorized by law.
- **Health Oversight Activities.** The Plan may disclose medical information about you to a health oversightagency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitorthe health care system, government programs, and compliance with civil rights laws.
- **Lawsuits and Disputes.** The Plan may disclose medical information about you in response to a court order, administrative order, subpoena, discovery request, or other lawful procedure. The Plan will only disclose your medical information if efforts have been made to inform you about the request or to obtain a protective order with respect to your medical information.
- **Law Enforcement.** The Plan may disclose medical information about you if asked to do so by a law enforcement official (1) in response to a court order, subpoena, warrant, summons, or similar process; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) about the victim of acrime, if under certain limited circumstances, you are the victim and the Plan is unable to obtain the your agreement; (4) about a death that the Plan believes may be the result of criminal conduct; or (5) about criminal conduct.
- **Coroners, Medical Examiners, and Funeral Directors.** The Plan may release medical information aboutyou to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. The Plan may also release medical information about you to afuneral director, as necessary to carry out the director's duties.
- **National Security and Intelligence Activities.** The Plan may release medical information about you toauthorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.
- **Research.** The Plan may disclose medical information about you to researchers, when individual identifiers have been removed or when an institutional review board or privacy board has reviewed the research proposal and established protocols to ensure the privacy of the requested information and approves the research.
- **Personal Representatives.** The Plan will disclose medical information about you to individuals you have authorized to be or individuals designated as your personal representative or equivalent (such as your power of attorney), so long as you provide the Plan with a written authorization and any supporting documents (such as a power of attorney). However, the Plan is not required to disclose information to a personal representative if the Plan reasonably believes that (1) you have been or may be subject to domestic violence, abuse, or neglect by such person, or (2) treating such person as your personal representative could endanger you, and (3) in the exercise of professional judgment, the Plan decides that it is in your best interests not to treat such person as your personal representative.
- **Spouses and Other Family Members.** The Plan will send all mail related to all covered individuals to the applicable employee or retiree, except for limited circumstances. However, if a covered individual requests restrictions or confidential communications (see below) and the Plan has agreed to such request, the Plan will send mail in accordance with such request.

- **Underwriting.** The Plan may use or disclose medical information about you for underwriting purposes, but the Plan is prohibited from using or disclosing any genetic information about you for such purposes.

• Authorizations

Other uses and disclosures of your medical information not covered by this Notice or the laws that apply to the Plan will be made only with your written authorization. If you provide the Plan with written authorization to use or disclose medical information about you (for a purpose that requires that authorization), you may revoke that authorization, in writing, at any time. If you revoke your authorization, thereafter the Plan will no longer use or disclose medical information about you for the reasons covered by your written authorization. However, the revocation is only effective with regard to future uses and disclosures. The Plan is unable to undo any uses or disclosures that were made before such revocation.

The Plan will not use or disclose medical information about you without a written authorization from you in the following specific situations:

- **Psychotherapy Notes.** The Plan will not use or disclose psychotherapy notes about you without a written authorization, unless (a) the disclosure is to the originator of the notes for treatment purposes, (b) the use or disclosure is to defend the Plan in a legal action or proceeding brought by you, (c) the useor disclosure is required by the Secretary of the Department of Health and Human Services, or (d) the use or disclosure is permitted because the disclosure is (i) required by law, (ii) to a health oversight agency for oversight activities authorized by law related to the originator of the notes, (iii) to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law, or (iv) to prevent or lessen a serious or imminent threat to the health or safety of a person or the public, where such disclosure is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.
- **Marketing.** The Plan will not use or disclose medical information about you for marketing purposes without a written authorization, unless the communication is (a) a face-to-face communication by the Plan to you, or (b) a promotional gift of nominal value from the Plan to you. Further, the Plan will not receive financial remuneration from a third party with respect to any marketing unless your authorization state that remuneration is involved.
- **Sale.** The Plan will not sell medical information about you without a written authorization that includes a statement that such disclosure will result in remuneration to the Plan.

• Your Rights Regarding Medical Information About You

You have the following rights regarding medical information about you:

- **Right to Access.** You have the right to inspect and obtain a copy of medical information that we maintain about you in certain records maintained by the Plan. The Plan is required to disclose to you medical information contained in your medical records; billing records; enrollment, payment, claims adjudication, and case or medical management record systems; and any other records used to make decisions regarding your health care benefits.

  To inspect and obtain a copy of your medical information, you must submit a written request to the Plan's third-party administrator or your insurance carrier listed in the applicable Summary Plan Description or Summary of Material Modification. If you request a copy of your medical

information, a reasonable fee may be charged for the costs of copying, mailing, or supplies associated with your request.

Your request to inspect and copy may be denied in certain limited circumstances. If you are denied access to your medical information, you may request that the denial be reviewed by submitting a request to the Plan's Privacy Official at: Plan Privacy Official, Ethics & Compliance Group, The Procter & Gamble Company, 1 Procter & Gamble Plaza, C9-134B, Cincinnati, OH 45202.

- **Right to Amend.** If you believe that the Plan's medical information about you is incorrect or incomplete, you may ask to amend the information. You have the right to request an amendment for as long as the information is kept by or for the Plan.

To request an amendment, you must submit a written request to the Plan's third-party administrator or your insurance carrier listed in the applicable Summary Plan Description or Summary of Material Modification. In addition, you must provide a reason that supports your request.

Your request for an amendment may be denied if it is not in writing or does not include a reason to support the request. In addition, your request may be denied if you ask to amend medical information that:

- was not created by the Plan, unless you provide a reasonable basis to believe that the person or entity that created the information is no longer available to make the amendment;
- is not part of the medical information kept by the Plan;
- is not part of the medical information which you would be permitted to inspect and copy; or
- is already accurate and complete.

If the Plan denies your request, you have the right to file a statement of disagreement with the Plan's decision, and we may give a rebuttal to your statement. If you file a statement of disagreement, the Plan will maintain your statement of disagreement and the Plan's rebuttal (if any) as part of your medical information.

- **Right to an Accounting of Disclosures.** For most disclosures of your medical information other than those specified below, you have the right to request an "accounting of the disclosures" we made in the six years prior to the date of your request. An accounting of disclosures will not include (1) disclosures made for purposes of treatment, payment, or health care operations; (2) disclosures made directly to you; (3) disclosures made pursuant to your written authorization; (4) disclosures made to friends or family involved in your care, in your presence or because of an emergency; (5) disclosures for national security purposes; and (6) disclosures incidental to otherwise permissible disclosures. The right to receive an accounting of disclosures of your medical information is subject to certain other exceptions, restrictions, and limitations.

  To request an accounting of disclosures, you must submit your request in writing to the third-party administrator or your insurance carrier listed in the applicable Summary Plan Description or Summary of Material Modification. Your request must state a time period that may not be longer than six years prior to the date of your request. The first accounting you request within a 12-month period will be provided free of charge, but you will be charged for the cost of providing additional accountings within that time period. You will be notified of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

- **Right to Request Restrictions on Certain Uses and Disclosures.** You have the right to request that the Plan restrict certain uses and disclosures of your medical information for treatment,

payment, or health care operations. You also have the right to request that the Plan limit the medical information about you that the Plan discloses to someone who is involved in your care or the payment for your care, such as a family member or friend.

Except as provided in the next paragraph, the Plan is not required to agree to your request. If the Plan agrees to your request, the Plan will comply with your request until you revoke it or the Plan notifies you that the Plan no longer agree to such restriction or limitation.

The Plan will comply with a restriction request if the disclosure of your medical information is (1) to another health plan and is for the purpose of carrying out payment or health care operations (but not treatment), (2) not otherwise required by law, and (3) pertains solely to a health care item or service for which you, or a person on your behalf, has paid out-of-pocket in full.

To request such restrictions, you must make your request in writing to the third-party administrator or your insurance carrier listed in the applicable Summary Plan Description or Summary of Material Modification. In your request, you must state (1) what information you want to limit; (2) whether you want to limit the Plan's use, disclosure, or both; and (3) to whom you want the limits to apply (for example, disclosures to your spouse).

Right to Request Confidential Communications. You have the right to request that the Plan communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that the Plan only contact you at work or by mail.

To request confidential communications, you must make your request in writing to the third-party administrator or your insurance carrier listed in the applicable Summary Plan Description or Summary of Material Modification. The Plan will not ask you for the reason for your request. Your request must specify how or where you wish to be contacted. The Plan will accommodate all reasonable requests if you clearly provide information that the disclosure of all or part of your medical information could endanger you.

- **Right to a Paper Copy of This Notice.** You have the right to receive a paper copy of this Notice at any time, even if you have previously agreed to receive this Notice electronically. To obtain a paper copy of this Notice, please request one in writing from U.S. Benefits Services.

• Changes to this Notice

The Plan reserves the right to change this Notice. The Plan reserves the right to make the revised or changed Notice effective for medical information that the Plan already has about you as well as any medical information about you the Plan receives in the future. P&G provides an online version of the current Notice of Privacy Practices on P&G's website, at https://privacypolicy.pg.com/policy/hipaaNOPP.

The effective date of the Notice will be listed on the first page of the Notice.

- ## Complaints

If you have questions or would like additional information about our privacy practices, you may contact the Plan's Privacy Official by sending an email to corporateprivacy.im@pg.com. If you believe your privacy rights have been violated, you may file a complaint with the Plan or with the Secretary of the Department of Health and Human Services. To file a complaint with the Plan, contact the Director, U.S. Health and Wellness Benefits, GBS-My P&G Services (or equivalent) at:

Director
U.S. Health and Wellness Benefits, GBS-My P&G Services
The Procter & Gamble Company
2 Procter & Gamble Plaza, TE-3
Cincinnati, OH 45202

You also may file a complaint with the Plan's Privacy Official at: Plan Privacy Official, Ethics & Compliance Group, The Procter & Gamble Company, 1 Procter & Gamble Plaza, C9-134B, Cincinnati, OH 45202.

All complaints must be submitted in writing. You will not be penalized, or in any other way retaliated against, for filing a complaint with the Plan or the Secretary of the Department of Health and Human Services.

- ## Privacy Official

The Global Privacy Officer of The Procter & Gamble Company is the Plan's Privacy Official for the Plan. Please check www.pg.com/privacy for more information.

- ## Contact Information

Global Privacy Officer
Ethics & Compliance Group
The Procter & Gamble Company
1 Procter & Gamble Plaza, C9-134B
Cincinnati, OH 45202