MARATHON PETROLEUM

HIPAA PRIVACY POLICY

Effective September 1, 2023

MARATHON PETROLEUM HIPAA PRIVACY POLICY

I. PURPOSE

The Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act (collectively referred to here as "HIPAA") are federal laws that, in relevant part establish rules (the "Privacy Rule") regarding the use of protected health information ("PHI") created or received by group health plans (each a "covered entity" for purposes here). The Privacy Rule requires covered entities to implement policies and procedures to ensure compliance with the Privacy Rule.

This Marathon Petroleum HIPAA Privacy Policy ("Policy") designed to comply with the HIPAA federally mandated privacy and confidentiality rules and requirements for the group health plans sponsored by Marathon Petroleum Company LP ("MPC") (the "Plans"). This Policy is intended to ensure that the Plans minimize the amount of PHI used and disclosed by or to the Plans by:

- Limiting persons who have access to PHI;
- Describing proper handling and usage of PHI:
- Describing other requirements for compliance with the Privacy Rule.

A separate Notice of Privacy Practices is a part of this Policy and can be found on the MPC Benefit Website at www.myMPCbenefits.com.

II. SCOPE

This Policy applies to the following Plans sponsored by MPC and describes how protected health information ("PHI", as defined under the Privacy Rule) under these Plans may be used and disclosed and how an individual can access this information:

- Marathon Petroleum Health Plan
- Marathon Petroleum Retiree Health Plan
- Marathon Petroleum Dental Plan
- Marathon Petroleum Pre-65 Retiree Dental Plan
- Marathon Petroleum Vision Plan
- Marathon Petroleum Pre-65 Retiree Vision Plan
- Marathon Petroleum Employee Assistance Program
- Marathon Petroleum Health Care Flexible Spending Account Plan
- Marathon Petroleum Exchange Health Reimbursement Account Plan

III. DEFINITIONS

1. **Authorization**. Allows the use and disclosure of protected health information for purposes other than treatment, payment and health care operations by both the covered entity requesting the authorization and a third party.
2. **Breach**. Unauthorized acquisition, access, use, or disclosure of unsecured PHI that compromises the security or privacy of the information.
3. **Business Associate**. An entity (not a member of a covered entities workforce) that creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA on behalf of a covered entity. This includes any entity involved in a function or activity that involves the use or disclosure of individually identifiable health information,

including claims processing or administration; data analysis, processing or administration; utilization review quality assurance; billing; benefit management; practice management and re-pricing; legal; actuarial; accounting; consulting; data aggregation management; administrative; accreditation or financial services.

4. **Company**. MPC and, where the context requires, any of its affiliates.
5. **Electronic Media**. Electronic storage material on which data is or may be recorded electronically, including devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet, intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, voice via telephone, and facsimile, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.
6. **Electronic Protected Health Information ("EPHI").** Protected health information that is transmitted by or maintained in Electronic Media.
7. **De-Identified Information**. Health information that does not identify an individual and reasonably cannot be used to identify an individual.
8. **Healthcare Operations**. Administrative, financial, legal and quality improvement activities of the Plans that are necessary to run their business and to support the core functions of treatment and payment.
9. **HIPAA**. As defined above.
10. **HIPAA Privacy Officer or Privacy Officer**. An individual designated by the Plans who is responsible for developing and implementing the privacy policies and procedures, monitoring compliance and overseeing training.
11. **HIPAA Security Officer**. An individual designated by the Plans who responsible for the development and implementation of the Plans' policies and procedures relating to security, including but not limited to this Policy. The Security Officer will coordinate the Plans' security activities with the Plans' Privacy Officer.
12. **HIPAA Security Standards**. HIPAA's security rule requires the Plan Sponsor to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the Plan Sponsor creates, receives, maintains, or transmits on behalf of the Plans, and as used here, "HIPAA Security Standards" means such rule's requirements as adopted by the Plan Sponsor.
13. **Payment**. Various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the health plan, and to obtain or provide reimbursement for the provision of health care. Example: Determining eligibility or coverage under a health plan and adjudicating claims.
14. **Personal Representatives**. A person authorized, under state or other law, to make health care decisions on the individual's behalf.
15. **Privacy Rule**. As defined above, and including the Standards for Privacy of Individually Identifiable Health Information promulgated under HIPAA at 45 Code of Federal Regulations Part 160 and Subparts A and E of Part 164 as in effect from time to time.
16. **Protected Health Information ("PHI")**. As defined above, health information that is created or received by the Plans, if the health information could be used to identify a specific individual, and relates to 1) the individual's physical or mental health condition, 2) the provision of health care, or 3) the payment for health care. Genetic information is considered PHI. Wherever PHI is referenced, EPHI is included by default.

17. **TPO**. Acronym for Treatment, Payment, and Healthcare Operations. This is used to describe the purposes for which PHI can be used.
18. **Treatment.** The provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health provider to another.

IV. GUIDELINES AND PROCEDURES

The following guidelines and procedures shall be applied to all PHI and any party granted access to PHI:

1. Minimum Necessary Standards:

When using or disclosing PHI or when requesting PHI from another entity, the Plans will make reasonable efforts not to use, disclose or request more than the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request, taking into consideration practical and technological limitations. This is defined as the "Minimum Necessary Standard."

The minimum necessary standard will not apply in the following situations:

- Disclosures to or requests by a health care provider for treatment;
- Uses or disclosures made to the individual;
- Disclosures made to the Secretary of the U.S. Department of Health and Human Services;
- Uses or disclosures that are required by law; and
- Uses or disclosures that are required for the Plan's compliance with legal regulations

<u>De-Identified Data</u>
This notice also does not apply to information that has been de-identified. De-identified information for which there is no reasonable basis to believe the information can be used to identify an individual is not considered individually identifiable health information. De-identified data can be used and disclosed, as needed, to conduct necessary business functions or activities.

The Plan may also use or disclose "summary health information" to the Plan Sponsor for obtaining premium bids or modifying, amending or terminating the Plan. Summary health information summarizes the claims history, claims expenses or type of claims experienced by individuals for whom the Plan Sponsor has provided health benefits under a Plan. In sharing summary data, the information is de-identified, and all identifying information is deleted in accordance with HIPAA.

2. HIPAA Privacy Officer:

In order to be in compliance with the Privacy Rule, the Plans need to designate a HIPAA Privacy Officer and a contact person or office. The Plans have designated the **MPC Benefits Policy Manager** to serve in both capacities. The Privacy Officer has, at minimum, the following tasks to oversee:

- Tracking all PHI;
- Making sure that legal issues are addressed;
- Coordinating with other employer functions;

- Setting up structures to ensure individual rights;
- Setting up a complaint process and sanctions;
- Developing overall privacy policies and procedures and the Notice of Privacy Practices;
- Developing a training program;
- Auditing and monitoring;
- Keeping up-to-date with the latest privacy developments; and
- Investigating a potential Breach of PHI and notifying individuals in case of a breach.

3. Business Associates:

The Privacy Officer will identify the Plan's Business Associates and have each sign a Business Associate Agreement. Business Associates, in general, are those entities, other than insurers or HMOs, which perform functions or activities on behalf of the Plans that involve the use or disclosure of PHI. PHI can be shared with a Business Associate applying the Minimum Necessary Standard.

The Privacy Officer may rely upon the Business Associates to perform their duties as outlined contractually and in the Business Associate Agreement, but will reserve the right to audit or otherwise oversee HIPAA Privacy and Security compliance. The Plans are not responsible for assuring that a Business Associate requests the minimum necessary information.

The Privacy Officer will receive reports of breaches of privacy or security from Business Associates and take corrective action when necessary.

<u>Authorized Contacts:</u>
Lists of authorized contacts for dealing with PHI will be exchanged between the Business Associates and the Plans. The personnel on these lists may be identified by title, department, or by name. The lists will be held by the Privacy Officer in a secure location. The lists will be used to identify authorized persons for discussing and receiving PHI.

The following organizations within MPC are authorized to have access to, use, or disclose PHI among Business Associates for legally permitted purposes or to carry out treatment, payment, and health care operations:

- HIPAA Privacy Officer
- HIPAA Security Officer
- MPC Payroll
- MPC Benefits Policy
- MPC Benefits Service Center
- MPC Workday/HR IT Support
- MPC HR Legal
- Business Associates
- MPC Plan Administrators and Assistant Plan Administrators

4. Uses and Disclosures of PHI:

The Plans will use protected health information to the extent of and in accordance with the uses and disclosures permitted by HIPAA and the Privacy Rule. Specifically, the Plans will use and disclose PHI for purposes related to health care treatment, payment for health care and health care operations as described below.

The Plans will disclose PHI only to the Plan Administrator and other members of the Company's workforce who are authorized to receive such PHI, and only to the extent and in the minimum amount necessary for that person to perform Plan administrative functions.

The Plans are permitted to use and disclose PHI without written authorization for certain legally permitted purposes or in certain situations, as described below. In all instances, the programs will limit the use or disclosure of PHI to the "minimum necessary" use or disclosure.

The Plan Sponsor has amended the respective Plan document to protect individual's PHI as required by federal law.

Uses and disclosures to carry out treatment, payment and health care operations
The Plans and their business associates will use PHI without consent, authorization, or an opportunity to agree or object to carry out treatment, payment and health care operations. The Plans also will disclose PHI to the Plan Sponsor and its subsidiaries for purposes related to treatment, payment and health care operations.

- ***Treatment*** is the provision, coordination or management of health care and related services. It also includes but is not limited to consultations and referrals between one or more of providers. For example, a Plan may disclose to a treating orthodontist the name of the treating dentist so that the orthodontist may ask for dental X-rays from the treating dentist.
- ***Payment*** includes but is not limited to actions to make coverage determinations and payment (including billing, claims management, subrogation, plan reimbursement, reviews for medical necessity and appropriateness of care and utilization review and pre-authorizations). For example, a Plan may tell a doctor whether an individual is eligible for coverage or what percentage of the bill will be paid by the Plan.
- ***Health Care Operations*** include but are not limited to quality assessment and improvement, reviewing competence or qualifications of health care professionals, underwriting, premium rating and other insurance activities relating to creating or renewing insurance contracts. It also includes disease management, case management, conducting or arranging for medical review, legal services and auditing functions including fraud and abuse compliance programs, business planning and development, business management and general administrative activities. For example, a Plan may use information about an individual's claims to refer them to a disease management program, project future benefit costs or audit the accuracy of its claims processing functions.

Other uses and disclosures that do not require authorization

1. When required by law,
2. When permitted for purposes of public health activities, including when necessary to report product defects, to permit product recalls and to conduct post-marketing surveillance. PHI may also be used or disclosed if there has been exposure to a communicable disease or are a risk of spreading a disease or condition, if authorized by law.
3. When authorized by law to report information about abuse, neglect or domestic violence to public authorities if there exists a reasonable belief that an individual may be a victim of abuse, neglect or domestic violence. In such case, the Plan will promptly inform the individual that such a disclosure has been or will be made unless that notice would cause a risk of serious harm. For the purpose of reporting child abuse or neglect, it is not necessary to inform the minor that such a disclosure has been or will be made. Disclosure may generally be made to the minor's parents or other representatives although there may be circumstances under federal or state law when the parents or other representatives may not be given access to the minor's PHI.
4. To a public health oversight agency for oversight activities authorized by law. This includes uses or disclosures in civil, administrative or criminal investigations; inspections; licensure or disciplinary actions (for example, to investigate complaints against providers); and other activities necessary for appropriate oversight of government benefit programs (for example, to investigate Medicare or Medicaid fraud).
5. When required for judicial or administrative proceedings. For example, PHI may be disclosed in response to a subpoena or discovery request provided certain conditions are met. One of those conditions is that satisfactory assurances must be given to the Plan that the requesting party has made a good faith attempt to provide written notice, and the notice provided sufficient information about the proceeding to permit individuals to raise an objection and no objections were raised or were resolved in favor of disclosure by the court or tribunal.
6. When required for law enforcement purposes (for example, to report certain types of wounds).
7. For law enforcement purposes, including for the purpose of identifying or locating a suspect, fugitive, material witness or missing person. Also, when disclosing information about an individual who is or is suspected to be a victim of a crime, but only if the individual agrees to the disclosure, or the covered entity is unable to obtain the individual's agreement because of emergency circumstances. Furthermore, the law enforcement official must represent that the information is not intended to be used against the individual, the immediate law enforcement activity would be materially and adversely affected by waiting to obtain the individual's agreement and disclosure is in the best interest of the individual as determined by the exercise of the Plan's best judgment.
8. When required to be given 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. Also, disclosure is permitted to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent.
9. The Plans may use or disclose PHI for research, subject to conditions.

10. When consistent with applicable law and standards of ethical conduct if the Plan, in good faith, believes 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 the disclosure is to a person reasonably able to prevent or lessen the threat, including the target of the threat.
11. When authorized by and to the extent necessary to comply with workers' compensation or other similar programs established by law. Except as otherwise indicated in this notice, uses and disclosures will be made only with written authorization subject to the right to revoke such authorization.
12. Where a participant is an organ donor, the Plans may release PHI to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.
13. Where a participant is a member of the armed forces, the Plans may release PHI about you as required by military command authorities. The Plans may also release PHI about foreign military personnel to the appropriate foreign military authority.
14. To authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.
15. If a participant is an inmate of a correctional institution or under the custody of a law enforcement official, the Plans may disclose PHI about the participant to the correctional institution or law enforcement official. This disclosure must be necessary (1) for the institution to provide the participant with health care; (2) to protect the participant's health and safety or the health and safety of others; or (3) for the safety and security of the correctional institution.
16. To researchers when: (1) the individual identifiers have been removed; or (2) when an institutional review board or privacy board has (a) reviewed the research proposal; and (b) established protocols to ensure the privacy of the requested information, and approves the research.
17. The Plans are required to disclose a participant's PHI to the Secretary of the U.S. Department of Health and Human Services when the Secretary is investigating or determining the Plans' compliance with the Privacy Rule.

<u>Uses and disclosures that require written authorization</u>

Prior authorization is required for any use or disclosure for purposes not described in this Policy or in the Notice of Privacy Practices. Therefore, except as described in this policy or the notice, the Plan will not use or disclose health information without written authorization. If an individual authorizes use or disclosure of health information for another purpose, the authorization may be revoked in writing at any time. If an authorization is revoked, the Plan will no longer be able to use or disclose health information for the reasons covered by the written authorization, though it will be unable to take back any disclosures that have already made with permission.

Prior authorization is required for most uses and disclosures of psychotherapy notes. As such, written authorization is required before the Plan will use or disclose psychotherapy notes from a psychotherapist. Psychotherapy notes are separately filed notes about conversations with a mental health professional during a counseling session. They do not include summary information about mental health treatment. The Plan may use and disclose such notes when needed by the Plan to defend against litigation that is filed.

Uses and disclosures that require an opportunity to agree or disagree prior to use or release

Disclosure of PHI to family members, other relatives and close personal friends is allowed if:

- The information is directly relevant to the family or friend's involvement with care or payment for that care; and
- Disclosure has been agreed to or there was no objection when given an opportunity.

Note: Consent may be obtained retroactively in emergency situations.

Prohibited Uses and disclosures of PHI

The Plans are prohibited from using or disclosing PHI that is genetic information for underwriting purposes.

Note: Use and disclosure of PHI may be required by the Secretary of the U.S. Department of Health and Human Services to investigate or determine a Plan's compliance with the privacy regulations.

In the event that any member of the Company's workforce uses or discloses PHI other than as permitted by the terms of the Plan regarding PHI, or this Policy, or as otherwise permitted under the Privacy Rule (collectively, the "HIPAA Privacy Standards"), the incident shall be reported to the Privacy Officer. The Privacy Officer shall take appropriate action, as described herein.

5. General Precautions and Handling Procedures:

In order to protect the privacy and ensure adequate security of PHI, as required by HIPAA, the Company has agreed to:

- Not use or further disclose PHI other than as permitted or required by the Plan document or as required by law, including HIPAA privacy standards;
- Implement reasonable and appropriate administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of EPHI that the Company creates, receives, maintains or transmits on behalf of the Plan;
- Ensure that the adequate separation between the Plan and the Company described above is supported by reasonable and appropriate security measures;
- Ensure that any agents, including a subcontractor, to whom it provides PHI received from the Plan agree to the same restrictions and conditions that apply to the Company with respect to such PHI;
- Ensure that any agent to whom it provides EPHI shall agree, in writing, to implement reasonable and appropriate security measures to protect the EPHI;
- Not use or disclose PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the Company;
- Report to the Plan any PHI use or disclosure that is inconsistent with the uses or disclosures provided for of which it becomes aware;
- Report to the Plan Administrator any security incident of which it becomes aware;
- Make PHI available to an individual in accordance with HIPAA's access requirements;
- Make PHI available for amendment and incorporate any amendments to PHI in accordance with HIPAA;

- Make available the information required to provide an accounting of disclosures;
- Make internal practices, books and records relating to the use and disclosure of PHI received from the Plan available to the Secretary of the U.S. Department of Health and Human Services for the purposes of determining the Plan's compliance with HIPAA;
- If feasible, return or destroy all PHI received from the Plan that the Company still maintains in any form, and retain no copies of such PHI when no longer needed for the purposes for which disclosure was made (or if return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction infeasible);
- To use reasonable and appropriate security measures to protect the security of all PHI, including EPHI, and to support the separation between the Plan and the Company, as needed to comply with the HIPAA Security Standards.

The table below lists various ways that PHI may be handled along with the precaution that should be taken to ensure the privacy of the PHI.

Use	Precaution
Oral Communications	When discussing PHI on the phone or in person, reasonable efforts need to be taken so the conversation is not overheard. For example, use a lowered voice and avoid public areas. Use of a speakerphone while outside a closed conference room is undesirable.
Email	Use of email is permissible to exchange PHI; however, email distribution lists should be limited to "need to know" only. CC only those who need the information to accomplish the intended task. Think about whether parts of the email that identify the individual or the health condition can be deleted. Emails sent outside the Company should be sent encrypted or secured via a password that is delivered by phone.
Fax	Notify the fax recipient prior to sending fax and ensure the receiving fax is in a secure location and/or will be picked up promptly.
Paper Document Storage	Documents containing PHI should be stored in locked file cabinets or desks when not in a restricted access room. All documentation should be secured at the end of the day and should not be left out in the open unattended. If an office is considered high risk for storage of HIPAA documentation, it should be locked for restricted access.
Paper Document Disposal	Documents containing PHI must be disposed via the confidential document disposal process. This includes the use of shred boxes.
Terminating Employees	Employees with access to PHI must surrender their computer systems (hard drives) to IT upon terminating. IT has a secure destruction process to eliminate data from hard drives (i.e. by magnetically wiping hard drives, physically destroying them or overwriting the media).
Transferring Employees	Employees transferring to a new position that no longer requires access to PHI must delete all PHI from their desktop or laptop hard drives.
Verification of Identity and Authority Before Disclosure	Before any disclosure of PHI, the identity of the person who will be receiving the PHI and their authority for access to PHI must be verified.

Special Handling Procedures:

Use	Precaution
Appeals	Appeals are stored in locked files and are only seen by those involved in appeals decision making or administration.
Third Party Requests	Family members or other non-owners of PHI requesting information on behalf of a PHI owner must provide a valid written authorization from that PHI owner.

More information can be obtained regarding the use of PHI under HIPAA and the establishment of a HIPAA Security Officer from the Notice of Privacy Practices available at www.myMPCbenefits.com/documents/mpc-hipaa-notice-of-privacy-practices.pdf.

6. Third Party Requests for PHI:

An authorization form is required whenever a third party (for example, an employee's spouse) requests another person's PHI.

A person may authorize the release of his/her PHI to a specified individual by completing an ***Authorization for Use or Disclosure of Protected Health Information*** form. Only the PHI specified in the authorization form may be disclosed to the individual named on such form and the form must be completed before the information can be disclosed. The form must be maintained on file through the expiration date. In addition, information cannot be released by the Plans or by any Business Associate of the Plans for marketing purposes without the permission of each participant.

The ***Authorization for Use or Disclosure of Protected Health Information*** form is a custom document that the Plans tailored to the specifications of the Privacy Rule. Its key features are a finite life (no more than 180 days) and a limitation of access to particular PHI (versus a general waiver). Also, a person has the right to revoke his/her authorization at any time, ceasing the disclosure of PHI to the third party. Such a revocation should be in writing.

Under the Privacy Rule, the Plans have the regulatory authority to use and disclose protected health information for TPO purposes without obtaining the individual's authorization.

For dependents over age 18, the Plans will disclose information to a parent or guardian unless the dependent has returned the ***Request to Restrict Use or Disclosure of Protected Health Information*** form that was included with their notification of the Plans' Notice of Privacy Practices.

The ***Authorization for Use or Disclosure of Protected Health Information*** form and the ***Request to Restrict Use or Disclosure of Protected Health Information*** form are located online at www.myMPCbenefits.com.

Authorizations used prior to April 14, 2003 are not valid.

7. HIPAA Notification Procedures:

The following table outlines the procedures for distributing the Notice of Privacy Practices to different categories of Plan participants.

Category	Distribution
New hires	Notice included in benefits enrollment packet
Spouses and adult children of new hires	Notice sent to home during the first month of employment of the new hire
New spouse or newly acquired dependent child over the age of 18 of current employee	Notice distributed to home when spouse/dependent added to the system
Dependent children of current employees turning age 18	Notice distributed to home the month prior or early in the month of 18th birthday
All Plan participants	Notice distributed by mail every three years; any time Notice is materially revised, the revised Notice will be posted on the benefits website.

8. Training:

Initial training concerning the Privacy Rule and the appropriate handling of PHI will be provided when an employee takes a position that requires the handling of PHI. The training will be required to be renewed annually.

Training will be available through a computer-based training course and also through formal classroom training (when requested). Employees' attendance at the training will be recorded and each employee taking the training will be required to pass a test.

9. Compliance and Sanctions for Non-Compliance:

The Plans are required by law to maintain the privacy of PHI and provide individuals with a notice of the practices in place to do so. In accordance with the Privacy Rule compliance requirement, these updated privacy practices are effective September 1, 2023.

The Plans are required to comply with the terms of this Policy. However, the Plan Sponsor reserves the right to change a Plan's existing privacy practices and apply changes as required under legislation relating to the privacy and security of PHI. The Plan Sponsor also reserves the right to have a Plan apply any such changes to any PHI received or maintained prior to the above date.

Violation of or noncompliance with these guidelines is grounds for discipline, at the Company's discretion, ranging from oral or written warning up to and including termination.

10. Change in privacy practices

If a privacy practice or the Notice of Privacy Practices has a material change, information regarding the change will be posted to the benefits website. In addition, a revised copy of the Notice of Privacy Practices will be provided, as required, to all past and present participants and beneficiaries for whom an affected Plan still maintains PHI.

V. INDIVIDUAL RIGHTS

An individual has certain rights in regard to their PHI. These rights include:

Right for Access to PHI
Upon request, the Plan is required to give access to certain PHI in order to inspect and copy it. If PHI is maintained electronically, it must provide access to the electronic information in the electronic form and format requested. If the form requested is not readily producible, another readable, electronic format must be offered.

Right to Request Restrictions on PHI Uses and Disclosures
An individual may request the Plan to restrict uses and disclosures of PHI to carry out TPO, or to restrict uses and disclosures to family members, relatives, friends or other persons identified who are involved in the care or payment for care. The Plan will accommodate reasonable requests to receive communications of PHI by alternative means or at alternative locations.

The disclosure of PHI to a Plan may be restricted if the disclosure is for one of the TPO activities stated above, is not required by law, and pertains solely to a health care item or service for which the individual (or someone on behalf of the individual) has paid out-of-pocket in full.

An individual or their personal representative will be required to complete a form to request restrictions on uses and disclosures of PHI.

Right to Inspect and Copy PHI
An individual has a right to inspect and obtain a copy of their PHI contained in a designated record set, for as long as the Plan maintains the PHI. PHI for this purpose includes all individually identifiable health information transmitted or maintained by the Plan, regardless of form.

The "designated record set" includes the medical records and billing records about individuals maintained by or for a covered health care provider; enrollment, payment, billing, claims adjudication and case or medical management record systems maintained by or for a Plan; or other information used in whole or in part by or for the covered entity to make decisions about individuals. Information used for quality control or peer review analyses and not used to make decisions about individuals is not in the designated record set.

The requested information will be provided within 30 days if the information is maintained on site or within 60 days if the information is maintained offsite. A single 30-day extension is allowed if the Plan is unable to comply with the deadline. An individual of their personal representative will be required to complete a form to request access to the PHI in a designated record set.

If access is denied, a written denial setting forth the basis for the denial, a description of how one may exercise those review rights as well as a description of how one may complain to the Secretary of the U.S. Department of Health and Human Services will be provided.

Right to Amend PHI
An individual has the right to request the Plan to amend PHI or a record in a designated record set for as long as the PHI is maintained in the designated record set. The Plan has 60 days after the request is made to act on the request. A single 30-day extension is allowed if the

Plan is unable to comply with the deadline. If the request is denied in whole or in part, the Plan must provide the individual with a written denial that explains the basis for the denial. A written statement disagreeing with the denial may be submitted and that statement may be included with any future disclosures of PHI.

Requests for amendment of PHI in a designated record set must be made to the HIPAA Privacy Officer. An individual or their personal representative will be required to complete a form to request amendment of the PHI in a designated record set.

Right to Receive an Accounting of PHI Disclosures

Upon request, the Plan will also provide an accounting of disclosures by the Plan of PHI during the six years prior to the date of the request. However, such accounting need not include PHI disclosures made:

(1) to carry out TPO;
(2) to individuals about their own PHI; or
(3) prior to the compliance date.

If the accounting cannot be provided within 60 days, an additional 30 days is allowed if the individual is given a written statement of the reasons for the delay and the date by which the accounting will be provided. If an individual requests more than one accounting within a 12-month period, the Plan will charge a reasonable, cost-based fee for each subsequent accounting.

Requests for Access, Restriction, Review/Amendment, or Account of Disclosures of PHI

To invoke any of the above rights, the individual must submit a written request to the HIPAA Privacy Officer. The request should include:

1) The individual's name
2) A brief description of the request
3) Contact information for the individual (phone number and/or email) with preferred method of contact.

Requests must be directed to:

MPC Benefits
Attn: HIPAA Privacy Officer
539 South Main St.
Findlay, OH 45840
E-mail: privacy@MarathonPetroleum.com

Right to Receive Notice of a Breach

Individuals have a right to receive a notification of any breach of individual unsecured PHI.

Right to File a Complaint

Any employee may submit a written complaint or grievance to the HIPAA Privacy Officer upon observing a breach of the HIPAA Privacy requirements. Employees of Business Associates are required to inform the Privacy Officer of breaches of the Privacy Rule on the part of the Business Associate. The Privacy Officer will maintain a log of complaints or grievances and their resolutions.

A complaint may also be filed with the Secretary of the U.S. Department of Health and Human Services, Hubert H. Humphrey Building, 200 Independence Avenue S.W., Washington, D.C. 20201.

As required by the Privacy Rule, MPC and its subsidiaries and the Plans will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

- Individuals who exercise their rights under these Policies and Procedures, including individuals who file complaints with the Privacy Officer.
- Any person, including an individual, who files a complaint with the Secretary of Health and Human Services under HIPAA, testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under HIPAA, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of HIPAA.

For additional information about individual rights in regard to PHI, please refer to the Notice of Privacy Practices, which can be found online at www.myMPCbenefits.com. ***Upon request, a paper copy of the Notice will be provided or an electronic copy will be provided via e-mail.***

VI. PERSONAL REPRESENTATIVE

In situations where an individual is legally or otherwise incapable of exercising privacy rights, or simply chooses to designate another to act on his or her behalf, the rules extend these rights to the individual's "personal representative," defined as a person authorized, under state or other law, to make health care decisions on the individual's behalf.

To the extent that a person is recognized as an individual's personal representative, the person may receive the individual's PHI and authorize other PHI uses and disclosures. The personal representative also may exercise rights such as accounting and amendment.

The Plans must verify the authority of a person who claims to be a personal representative. The instrument granting authority does not have to specifically address health information, as long as it grants authority to make health-related decisions for an individual. To authorize a personal representative, complete the ***Appointment of Personal Representative for Access to PHI Under HIPAA*** form, which can be found online at www.myMPCbenefits.com.