MARATHON PETROLEUM

HIPAA SECURITY POLICY

Effective September 1, 2023

MARATHON PETROLEUM HIPAA SECURITY POLICY

I. PURPOSE

The Health Insurance Portability and Accountability Act (“HIPAA”) and the Health Information Technology for Economic and Clinical Health Act (collectively referred to here as “HIPAA”) are federal laws that establish standards (the “Security Rule”) for the security of electronic protected health information (“ePHI”) created or received by group health plans (each such plan is a “covered entity” or “CE” for purposes here).

The Security Rule requires that each covered entity engaged in the electronic maintenance or transmission of ePHI assess the potential risks and vulnerabilities to such information. The Security Rule also requires the CE to develop, implement, and maintain appropriate security measures to protect that information and to document these measures and keep them current and up-to-date, such as, through the implementation of policies and procedures to ensure compliance with the Security Rule.

This Marathon Petroleum HIPAA Security Policy (“Policy”) is intended to comply with the Security Rule and covers these areas:

1. Administrative Safeguards
2. Physical Safeguards, and
3. Technical Safeguards.

II. SCOPE

This Policy applies to the following health plans sponsored by Marathon Petroleum Company LP (“MPC”) (the “Plans”):

- 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

This Policy describes how protected health information (“PHI”) under the Plans will be protected.

III. ORGANIZATIONAL REQUIREMENTS

1. ***Develop and Maintain Business Associate Contracts*** – The Plans have Business Associate agreements with all vendors who provide services to the Plans.
2. ***Plans Amended for Compliance*** – The Plan documents for the Plans have been amended to provide that each Plan sponsor will reasonably and appropriately safeguard ePHI created, received, maintained, or transmitted to or by the Plan sponsor on behalf of the Plans.

3. ***Policies and Procedures*** – Both the Marathon Petroleum HIPAA Privacy Policy and this Policy have been drafted, reviewed and adopted. The documents will be reviewed annually by the HIPAA Privacy Officer and HIPAA Security Officer.

IV. DEFINITIONS

1. **Access.** The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.
2. **Administration Safeguards.** Administrative actions, policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of the covered entity's workforce in relation to the protection of that information.
3. **Authentication.** The corroboration that a person is the one claimed.
4. **Authorization.** Allows the use and disclosure of PHI for purposes other than treatment, payment and health care operations ("TPO") by both the covered entity requesting the authorization and a third party.
5. **Availability.** The property that data or information is accessible and useable upon demand by an authorized person.
6. **Breach.** Unauthorized acquisition, access, use, or disclosure of unsecured PHI that compromises the security or privacy of the information.
7. **Business Associate.** An entity (not a member of a covered entity's workforce) that creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA on behalf of a covered entity. 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.
8. **Company**. MPC and, where the context requires, any of its affiliates.
9. **Confidentiality.** The property that data or information is not made available or disclosed to unauthorized persons or processes.
10. **De-Identified Information**. Health information that does not identify an individual and reasonably cannot be used to identify an individual.
11. **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.
12. **Electronic protected health information (ePHI).** PHI that is transmitted by or maintained in electronic media.
13. **Encryption.** The sue of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
14. **Facility**. The physical premises and the interior and exterior of a building(s).

15. **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.
16. **HIPAA Security Officer**. The 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' HIPAA Privacy Officer.
17. **Individual.** The person who is the subject of protected health information.
18. **Information System.** An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.
19. **Integrity.** The property that data or information have not been altered or destroyed in an unauthorized manner.
20. **Malicious software.** Software, for example, a virus, designed to damage or disrupt a system.
21. **Password**. Confidential authentication information composed of a string of characters.
22. **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 plan, and to obtain or provide reimbursement for the provision of health care. Example: Determining eligibility or coverage under a plan and adjudicating claims.
23. **Personal Representatives.** A person authorized, under state or other law, to make health care decisions on the individual's behalf.
24. **Physical safeguards.** Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
25. **Privacy Rule**. As promulgated under HIPAA, 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.
26. **Protected Health Information ("PHI").** 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 the individual's physical or mental health condition, the provision of health care, or the payment for health care. Genetic information is considered PHI. Wherever PHI is referenced, ePHI is included by default.
27. **Security or Security Measures**. All of the administrative, physical, and technical safeguards in an information system.
28. **Security incident**. The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
29. **Technical safeguards**. The technology and the policy and procedures for its use that protect ePHI and control access to it.
30. **Use**. With respect to individually identifiable health information, use means the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.
31. **User**. A person or entity with authorized access.

32. **Workstation**. An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

V. GUIDELINES AND PROCEDURES

The following safeguards have been implemented to protect the security of PHI:

1. ADMINISTRATIVE SAFEGUARDS

MPC has developed the following processes and procedures for ensuring the security of PHI in regard to day-to-day operations. The focus is on managing the conduct of employees with access to ePHI and managing the selection, development, and use of security controls.

A. Security Management

- Risk Analysis – An assessment of the potential risks and vulnerabilities to the confidentiality, integrity, availability of ePHI held by the Plans is conducted regularly.
- Risk Management – The IT security measures that are in place are reviewed to make sure they are sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Rule. These measures are documented on the MPC IT Compliance TeamView and have standard review period which is established by the IT Governance Policy (IT-002).
- Sanction Policy – Sanctions for violation of various IT security measures are governed by Company Policy 6002 – Use of Information Systems.
- Information system activity review – All changes to the system are documented through the standard IT Change Management tool and are outlined in IT-015 Change Management Standard.

B. *Assigned Security responsibility* – Named a HIPAA Security Officer responsible for maintaining security and investigating any possible breach of unsecured PHI.

C. *Workforce security*

- Authorization and/or Supervision – Employees are not hired without an approved authorization and a vacant position that reports to a supervisor.
- Workforce Clearance Procedures – The employee's supervisor along with the data owner must approve all security requests through the security process, unless the security process is pre-approved through a documented process.
- Termination Procedures – Upon termination, the employee's PIC (Personal Identification Code) which allows access to the network is disabled, thereby shutting off access to all network applications.

D. *Information Access Management*

- Isolating Healthcare Clearinghouse functions – Not applicable to this Policy.

E. Access Authorization – This function is controlled through the CS Information Protection Policy (SC-011). There are various standards subordinate to the policy that govern specific aspects of security. A complete list of IT Policies and Standards is available on the MPC IT Compliance TeamView.

- Access Establishment and Modification – This function is controlled through the security-related IT Policies and Standards governed by CS-011.

F. *Security Awareness Training*

- Security Reminders – Standard approval requests and reviews are governed by the CS-011 Information Protection Policy.
- Protections from malicious Software – This function is governed by CS-064 Vulnerability and Patch Management Standard
- Log-In monitoring – This function is governed by CS-011 Information Protection Policy and its subordinate standards.

G. *Security Incident Procedures* – Response and reporting of security incidents are governed by CS-011 Information Protection Policy and its subordinate standards.

H. *Contingency Plan*

- Data Backup Plan – Backup plans are documented and retained at each appropriate data center, which are controlled by third parties.
- Disaster Recovery Plan – Disaster recovery plans are documented and retained at each appropriate data center, which are controlled by third parties.
- Emergency Mode Operation Plan – Emergency mode operation plans are documented and retained at each appropriate data center, which are controlled by third parties.
- Testing and Revision Procedures – These functions are controlled through IT Policies and Standards.
- Applications and Data Criticality Analysis – These functions are controlled through IT Policies and Standards.

I. *Evaluation* – Periodic Technical and Non-technical Evaluation of policies occurs on a regular basis.

J. *Business Associate Agreements* – Administrative safeguards are included in the business associate agreements that are retained in the office of the manger of Human Resources Services.

2. PHYSICAL SAFEGUARDS

The following security measures are in place to protect MPC's electronic information systems, as well as related buildings and equipment, from natural hazards, environmental hazards, and unauthorized intrusion.

A. *Facility Access Controls*

- Contingency Operations – Contingency operation plans are developed on a company-wide basis by a team established by the company to do so.
- Facility Security Plan – Company-wide security plans are maintained by the Corporate Health, Environment, Safety & Security organization and are documented on the Corporate Security TeamView.
- Access Control and Validation Procedures – These functions are maintained by Corporate Security.
- Maintenance records – Maintenance records are maintained by each data center. Data centers are controlled by third parties.

B. *Workstation use*

- Proper Functioning and Physical Attributes of Workstations – These functions are controlled through IT Policies and Standards.

- Physical Safeguards to Restrict access to Authorized Users – Workstations time out after a specified period of time and are locked until user enters PIC and Password.

C. Device and media controls

- Proper Disposal of PHI and hardware/software storing PHI – A special procedure has been implemented by SAIC to scrub all PCs that come from an HR or Health Services organization before the PCs are released from Marathon.
- Media Re-use – Media are not re-used without proper scrubbing.
- Accountability – Accountability for control of device and media resides with the management of each individual data center. Data centers are controlled by third parties.
- Data Backup and Storage – Data backup and storage occur according to the Plans maintained by each individual data center. Data centers are controlled by third parties.

3. TECHNICAL SAFEGUARDS

The following security measures specify how to use technology to protect EPHI, particularly controlling access to it.

A. Access Controls

- Unique User Identification – This function is controlled through CS-011 Information Protection Policy and its subordinate standards
- Emergency Access Procedure – This function is controlled through IT Corporate Directive.
- Automatic Logoff – Workstations time out after a period of time and are locked until the user enters PIC and Password.
- Encryption – Internal network not encrypted, but files sent outside the Company are encrypted or password protected.

B. *Audit Controls* – To record internal uses of PHI by a user, including:

- Updates are tracked by the system through the Workday audit log;
- Inquiries are controlled through security but not individually tracked.
- A list of job functions and the type of data they should be able to kept on file in the HIPAA Manual.
- The audit logs are reviewed on an ad hoc basis whenever a change is questioned.

C. *Integrity* – Authentication of Electronic PHI (ePHI) is controlled through IT security policies and standards.

D. *Person or entity authentication* – Authentication of the person or entity seeking access is controlled through CS-011 Information Protection Policy and its subordinate standards.

E. *Transmission security*

- Integrity Controls – Files transmitted to third parties containing ePHI utilize control totals and error reporting.
- Encryption – Files transmitted to third parties containing ePHI are encrypted using PGP.

VI. POTENTIAL BREACH OF UNSECURED PHI

A covered entity is required by law to notify individuals following a breach of unsecured PHI. Upon discovery of a breach, a Risk Analysis will be performed to determine the probability that the PHI has been compromised.

A thorough Risk Assessment will be performed to determine:

1. The nature and extent of PHI involved;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

A notification of breach will be made to the individuals impacted by the breach only if there is a high probability that the security of the PHI has been compromised. If the assessment concludes there was a low probability the PHI was compromised, a notice will not be made.

Documentation of the Risk Assessment and results will be kept on file.

VII. HIPAA SECURITY OFFICER

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

- Ensuring the confidentiality, integrity, and availability of all ePHI the Plans create, receive, maintain, or transmit;
- Protecting against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protecting against any reasonable anticipated uses or disclosures of such information that are not permitted; and
- Ensuring compliance with the Security Rule by the workforce.

VIII. 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.

IX. COMPLIANCE AND SANCTIONS FOR NON-COMPLIANCE

In accordance with the Security Rule compliance requirement, this Policy was first effective April 20, 2005 and have thereafter been revised from time to time. This version of the Policy as stated here is effective September 1, 2023. 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.