HIPAA SECURITY STANDARDS:

EMPLOYEE INFORMATION SHEET

The purpose of this information sheet is to provide guidance regarding the handling of electronic protected health information ("ePHI").

All employees, contractors, or others, at all locations and operations of CITGO Petroleum Corporation and its subsidiaries ("CITGO") who may have authorized direct or indirect access to ePHI should pay particular attention to this information.

Definitions. To assist in your understanding, the following are definitions of terms that apply to this Employee Information Sheet:

"Covered Entity" means a health plan, health care provider, or health care clearinghouse; specifically the term "Covered Entity" refers to the CITGO Petroleum Corporation Medical, Dental and Life Insurance Program for Salaried Employees; and the CITGO Petroleum Corporation Medical, Dental and Life Insurance Program for Hourly Employees.

"Electronic Media" means (i) electronic storage material on which data is or may be recorded electronically, including, for example, 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 (ii) transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

"ePHI" or Electronic Protected Health Information means individually identifiable health information that is (i) transmitted by electronic media, or (ii) maintained in electronic media. However, ePHI does not include identifiable health information which is contained in employment records held by CITGO (e.g., information given to supervisors by employees, information given to Health Services, etc.).

"HIPAA Security Regulations" are those regulations established by the U.S. Department of Health and Human Services interpreting sections of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Security Regulations may be found at 45 C.F.R. Parts 160, 162, and 164.

"Workforce" means those employees who have authorized direct or indirect access to ePHI in the performance of work for a Covered Entity. Generally, this will include employees in the benefits department, as well as some employees in the information technology department, audit department, facilities department, the human resources department, the legal department and the benefits accounting department. If you have any questions as to whether your position is included, please ask your manager.

General Statement of Information about the impact of the HIPAA Security Regulations. The Covered Entity must (1) ensure the confidentiality, integrity, and availability of all ePHI it creates, receives, maintains, or transmits; (2) protect against any reasonable anticipated threats or hazards to the security or integrity of such information; (3) protect against any reasonably anticipated use or disclosure of ePHI which is not permitted or required under the HIPAA Privacy Regulations; and (4) ensure compliance with the HIPAA Security Regulations by its Workforce. Compliance requires the Covered Entity to implement:

Administrative Safeguards – those 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 and authorized access to the ePHI;

Physical Safeguards – those physical measures, policies, and procedures to protect the Covered Entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion; and

Technical Safeguards – the technology and the policy and procedures for its use that protect ePHI and control access to it.

If there are any specific policies or procedures, in addition to CITGO's other policies and procedures, to be used by the Workforce, they will be explained by management as needed.

HIPAA Security Official. CITGO has assigned responsibility for the development and implementation of the policies and procedures required by the HIPAA Security Regulations. This person, the HIPAA Security Official, can be reached at **HIPAARequest@CITGO.com**.

Security Complaints. The HIPAA Security Official shall be responsible for facilitating a process by which an individual may file a complaint regarding the handling of ePHI by the Covered Entity. The HIPAA Security Official shall be responsible for ensuring that the complaint and its disposition are appropriately documented and handled. To make a complaint regarding the handling of ePHI, you should submit the complaint by email to **HIPAARequest@CITGO.com** and include as many details as possible. You will receive a written response concerning your complaint.

Discipline and other Sanctions for Violations. CITGO will appropriately discipline and/or sanction any person who violates the security of ePHI based upon its discretion as to the nature and circumstances of the violation. Discipline may include discharge from employment.

Other Responses to Security Violations. CITGO will attempt to correct or mitigate any violation of the security of ePHI. The HIPAA Security Official shall be responsible for determining whether and to what extent correction or mitigation is warranted.

Non-Retaliation. CITGO will not retaliate against any employee for reporting any violation or suspected violation of the security of ePHI.

Questions. Questions or comments concerning this information should be directed to **HIPAARequest@CITGO.com**.