OCCIDENTAL BENEFITS DEPARTMENT POLICY

HIPAA Security Policies and Procedures

Applicable to Health Plans
Sponsored by Occidental Petroleum Corporation and its Subsidiaries and Affiliates

Compliance Dates:
April 20, 2005 (for HIPAA Security Requirements)
February 17, 2010 (for Breach Notification Requirements)
September 23, 2013 (for Modifications under the Final HIPAA Rule)

Effective Revision Date – October 1, 2017

HIPAA Security Policies and Procedures

Table of Contents

Sec.	Topic	Citation
1.6	Security Incident Procedures	45 CFR §164.308(a)(6)(i)
	1.6.1 Response and Reporting	45 CFR §164.308(a)(6)(ii)
1.7	Contingency Plan	45 CFR §164.308(a)(7)(i)(A) – (E)
	1.7.1 Data Backup Plan	45 CFR §164.308(a)(7)(ii)(A)
	1.7.2 Disaster Recovery Plan	45 CFR §164.308(a)(7)(ii)(B)
	1.7.3 Emergency Mode Operation Plan	45 CFR §164.308(a)(7)(ii)(C)
	1.7.4 Testing and Revision Procedures (A)	45 CFR §164.308(a)(7)(ii)(D)
	1.7.5 Applications and Data Criticality Analysis (A)	45 CFR §164.308(a)(7)(ii)(E)
2.0	**Physical Safeguards**	
2.1	Facility Access Controls	45 CFR §164.310(a)(1)
	2.1.1 Contingency Operations (A)	45 CFR §164.310(a)(2)(i)
	2.1.2 Facility Security Plan (A)	45 CFR §164.310(a)(2)(ii)
	2.1.3 Access Control and Validation (A)	45 CFR §164.310(a)(2)(iii)
	2.1.4 Maintenance Records (A)	45 CFR §164.310(a)(2)(iv)
2.2	Workstation Use	45 CFR §164.310(b)
2.3	Workstation Security	45 CFR §164.310(c)
2.4	Device and Media Controls	45 CFR §164.310(d)(1) - (2)(iv)
	2.4.1 Disposal	45 CFR §164.310(d)(2)(i)
	2.4.2 Media Re-Use	45 CFR §164.310(d)(2)(ii)
	2.4.3 Accountability (A)	45 CFR §164.310(d)(2)(iii)
	2.4.4 Data Backup and Storage (A)	45 CFR §164.310(d)(2)(iv)

Sec.	Topic	Citation
3.0	**Technical Safeguards**	
3.1	Access Control	45 CFR §164.312(a)(1)
	3.1.1 Unique User Identification	45 CFR §164.312(a)(2)(i)
	3.1.2 Emergency Access Procedure	45 CFR §164.312(a)(2)(ii)
	3.1.3 Automatic Logoff (A)	45 CFR §164.312(a)(2)(iii)
	3.1.4 Encryption and Decryption (A)	45 CFR §164.312(a)(2)(iv)
3.2	Audit Controls	45 CFR §164.312(b)
3.3	Integrity	45 CFR §164.312(c)(1)
	3.3.1 Mechanism to Authenticate ePHI (A)	45 CFR §164.312(c)(2)
3.4	Person or Entity Authentication	45 CFR §164.312(d)
	3.4.1 E-mail	
	3.4.2 Telephone	
	3.4.3 Recorded Message	
3.5	Transmission Security	45 CFR §164.312(e)(1)
	3.5.1 Integrity Controls (A)	45 CFR §164.312(e)(2)(i)
	3.5.2 Encryption (A)	45 CFR §164.312(e)(2)(ii)
4.0	**Breach of Unsecured PHI**	
4.1	Notification to Individuals	45 CFR §164.404
	Notification to the Media	45 CFR §164.406
	Notification to the Secretary	45 CFR §164.408
	Administrative Requirements	45 CFR §164.503

Appendix	Topic
Appendix A	Definitions of HIPAA Terms
Appendix B	Covered Entity List
Appendix C	Business Associate Inventory
Appendix D	Form of Business Associate Agreement
Appendix E	Notice of Privacy Rights and Practices
Appendix F	Complaints Log
Appendix G	Plan Document Language
Appendix H	HIPAA Non-Routine Disclosure Log
Appendix I	Training Documentation
Appendix J	Breach Notification Log

Introduction to Group Benefit Plan of Occidental Petroleum Corporation HIPAA Security Policies and Procedures

In compliance with the Health Insurance Portability and Accountability Act of 1996, as amended, (HIPAA), certain group health plans (collectively referred to herein as the "Plan") maintained by Occidental Petroleum Corporation or its subsidiaries and affiliates ("Employer" or "Plan Sponsor"), have established internal practices on how to handle Plan employees' Protected Health Information (PHI) and to safeguard the Confidentiality, Integrity and Availability of Plan employees' electronic PHI (ePHI).

HIPAA Background

Through HIPAA, the federal government has defined and standardized practices and procedures that describe how certain personal Health Information that is maintained by the Plan (called "Protected Health Information" or "PHI") may be used and disclosed and how Individuals can access their PHI and ensure that their rights are protected. This federal law:

- Requires the Plan to define the groups that review and handle PHI;
- Protects Individually Identifiable Health Information;
- Provides Individuals with the right to access their own PHI;
- Requires Authorization to use and disclose PHI; and
- Ensures participants receive adequate notice of their Privacy rights.

HIPAA does not apply to Health Information about employees that is developed or maintained by Occidental Petroleum Corporation or its subsidiaries and affiliates in the role as employer of the employees (*e.g.*, information gathered in relation to workers compensation claims or in approving a request for a Family Medical Leave of Absence). It applies only to Plan information.

Policy and Procedure Highlights

The objective of the practices outlined in this Security Document is to define how the Plan may handle and share PHI and how it has established reasonable and appropriate safeguards to ensure the Confidentiality, Integrity and Availability of Individuals' ePHI and to protect this information from reasonably anticipated improper or unauthorized access, alteration, deletion and transmission. A few highlights include:

- Administrative Safeguards, including an overview of the Plan's Security management process, Security Incident procedures, access management, and periodic evaluation policy;
- Physical Safeguards, including the Plan's Facility access controls, Workstation use and Security policies, and device and media controls;
- Technical Safeguards, including technology-based access and audit controls, Authentication methods, and data transmission and Integrity controls; and
- Training and awareness for employees who handle PHI and ePHI.

This Security Document along with the Occidental Petroleum Corporation HIPAA Privacy Policies and Procedures document (the "Privacy Document") represent Occidental Petroleum Corporations policies and procedures applicable to its Health Plans. The purpose is to

implement reasonable and appropriate policies and procedures to comply with HIPAA, including privacy, data security, HITECH and applicable rules and regulations thereunder.

It is important for you to read this document carefully and understand your role in handling and protecting PHI and ePHI under HIPAA. There is a Glossary of Terms and Definitions in Appendix A of this Security Document. Those Terms and Definitions are capitalized within this Security Document. Please refer to Appendix A for a complete description/definition of the capitalized terms whenever you see them in this Security Document.

TOPIC: Security Management Process
SUBJECT: Implement policies and procedures to prevent, detect, contain and correct Security violations.

EFFECTIVE DATE: April 20, 2005
REVISION DATES: October 1, 2017

POLICY STATEMENT:

The Plan will implement policies and procedures to prevent, detect, contain and correct Security violations. These policies will include the following HIPAA Implementation Specifications:

1.1.1 Risk Analysis – an accurate and thorough assessment of the potential risks and vulnerabilities to the Confidentiality, Integrity, and Availability of the Plan's ePHI will be conducted.

1.1.2 Risk Management – sufficient Security Measures to reduce the risks and vulnerabilities to the Plan's ePHI to a level sufficient to comply with the HIPAA Security Rule will be implemented.

1.1.3 Sanctions – appropriate Sanctions against Workforce members who fail to comply with these policies and procedures will be applied.

1.1.4 Information System Activity Review – records of Information System activity will be regularly reviewed by the Information Technology Group.

The Plan also specifically incorporates herein by reference those policies and procedures contained in the Information Technology (IT) Responsibilities Policy and the Digital Security Policy (together, the "IT Security Policies") and the Standard for IT Hardware Asset Management, the IT Hardware Asset Disposal Procedure, the IT Systems Disaster Recovery Standard, the Oxy Cyber Security Incident Response Plan, and the Standard for Smart Devise Use (together, the IT Guidelines")(the IT Security Policies and the IT Guidelines, collectively, the "IT Security Policies and IT Guidelines"), together with any amendments or revisions thereto. The HIPAA Security Officer or designee will be responsible for monitoring the Plan's Security procedures and practices internally on a periodic basis.

PROCEDURES:

1.1.1 Risk Analysis

As part of its initial HIPAA Security Rule risk analysis, the Plan will assess the technical and non-technical components of its Security environment as they related to ePHI, including hardware, software, system interfaces, data and information and people. All Information Systems that house ePHI, including all hardware and software that are used to collect, store, process, or transmit ePHI will be identified. Functions and ownership and control of Information System elements will be analyzed and verified as necessary.

The Plan also will review and make a reasoned, well-informed and good-faith determination to implement all applicable Standards and Implementation Specifications under the HIPAA Security Rule.

A Security Report will be created to summarize the findings of the risk analysis. This Security Report will be maintained by the HIPAA Security Officer and/or his/her designee for a period of not less than six (6) years from the date it was completed or last updated.

The Security Report will be reviewed periodically to assess the Plan's compliance with the Security Rule and will be updated as may be necessary. (See also, Evaluation Policy, Section 1.8).

1.1.2 Risk Management

The Plan will analyze the data collected during the risk analysis and identify the risks and vulnerabilities of any ePHI stored, processed or transmitted by the Plan.

The Plan will implement reasonable and appropriate Security Measures to reduce risks to the Confidentiality, Integrity and Availability of ePHI to a reasonable and appropriate level, taking into consideration the Plan's size, complexity, technical capabilities, risk analysis and the costs of Security Measures.

Security Measures which are implemented and/or adopted by the Plan will be documented in the Security Report and the effectiveness of those Security Measures will be reviewed and audited as part of periodic evaluations of the Plan's Security environment conducted by the HIPAA Security Officer or his/her designee.

1.1.3 Sanctions

The Plan has established policies and procedures regarding disciplinary actions which are communicated to all Individuals included in the Covered Entity. These policies and procedures will make Individuals aware that violations may result in notification to Law Enforcement Officials and regulatory, accreditation, and licensure organizations and will advise them that civil or criminal penalties may apply for the misuse, disclosure or misappropriation of Health Information.

Sanctions will be implemented for those employees who do not follow the outlined policies and procedures. This will be applied to all violations, not just repeat violations. These Sanctions will be supported, and may be supplemented in Occidental Petroleum Corporations and its subsidiaries and affiliates HIPAA Privacy Policy, and in all Business Associate agreements.

These employees will be made aware of what actions are prohibited and punishable. Training will be provided and expectations will be made clear so individuals are not sanctioned for doing things which they were not aware were wrong or inappropriate.

Individual Sanctions may include any of the following:

(a) Verbal warning;
(b) Re-Training and/or education;
(c) Notice of disciplinary action placed in personnel files; and
(d) Other Sanctions, up to and including, termination of employment

Business Associate Sanctions may include any of the following:

(a) Verbal warning;
(b) Implementation of contract provisions that include contract penalties;
(c) Termination of contract; and
(d) Notification to HHS

Specific Sanctions will be determined based on the nature of the violation, its severity and whether or not it was intentional. Sanctions will be applied uniformly across all job categories. All Sanctions will be documented, with documentation retained for a period of not less than six (6) years.

No Sanctions will be taken against any Individual who, in good faith, lodges a complaint with any entity regarding a Security Rule violation or who refuses to follow a policy or procedure which he or she believes, in good faith, violates the Security Rule.

The HIPAA Security Officer or designee will be responsible for notifying the Plan about Individuals who fail to comply with the Security policies. The HIPAA Security Officer or designee will assist with providing the necessary information to appropriately apply disciplinary action, including notification to Law Enforcement Officials and regulatory, accreditation, and licensure organizations.

Please refer to the section titled "*Safeguards, Sanctions Against Workforce Members*" of the Privacy Document.

1.1.4 Information Systems Activity Review

The HIPAA Security Officer or designee will be responsible for coordinating the Information System activity record review as it relates to the Plan's ePHI. Information System activity will be reviewed annually to detect or correct Security violations.

The Plan has the following capabilities for reviewing Information System activity:

(a) Access/Privilege reports;
(b) Security Incident logs;
(c) User life cycle management; and
(d) Other internal Security controls and monitoring tools.

Workforce members will be informed that records of Information System activity may be reviewed and can be used to investigate causes of reported or suspected Security Incidents or Security violations.

TOPIC: Assigned Security Responsibility
SUBJECT: Designation of a HIPAA Security Officer.

EFFECTIVE DATE: April 20, 2005
REVISION DATES: October 1, 2017

POLICY STATEMENT:

The Plan has identified and designated a HIPAA Security Officer who is responsible for the development and implementation of the Plan's Security policies and procedures. The Vice President, Human Resources has currently been designated the HIPAA Security Officer for the Plan.

The HIPAA Security Officer or designee will ensure a central point of accountability within the Plan for Security-related issues. The HIPAA Security Officer or designee is responsible for developing and implementing the policies and procedures for the Plan and for compliance with the HIPAA Security Rule.

PROCEDURES:

The HIPAA Security Officer and any designee will be trained and responsible for reviewing the Plan's Security program. The HIPAA Security Officer and/or designee will coordinate efforts across the Plan to identify key Security initiatives and standards including virus protection, Security monitoring, intrusion detection, and physical access control and Security of Health Information held by the Plan.

The HIPAA Security Officer, or a designee, will be responsible for:

(a) Conducting or overseeing employee Training;
(b) Establishing employee Sanctions for failure to comply with the Security Rule;
(c) Maintaining compliance records; and
(d) Monitoring the Plan's Security procedures and practices internally on a periodic basis and implementing changes as necessary.

TOPIC: Workforce Security
SUBJECT: Ensuring appropriate access and preventing inappropriate access to ePHI.

EFFECTIVE DATE: April 20, 2005
REVISION DATES: October 1, 2017

POLICY STATEMENT:

The Plan's HIPAA policies and procedures are designed to ensure that all members of the Workforce have appropriate access to ePHI and to prevent those members of the Workforce who do not require access to ePHI from obtaining such access. These policies will include addressing the following HIPAA Implementation Specifications:

1.3.1 Authorization and/or Supervision (A) – procedures for the authorization and/or supervision of Workforce members who work with ePHI or in locations where it may reasonably be anticipated to be accessed will be adopted.
1.3.2 Workforce Clearance Procedures (A) – procedures to determine that the access of a Workforce member to ePHI is appropriate will be implemented.
1.3.3 Termination Procedures (A) – procedures for terminating access to ePHI when the employment of a Workforce member ends will be implemented.

The Plan also specifically incorporates herein by reference those policies and procedures contained in the IT Security Policy, together with any amendments or revisions thereto.

PROCEDURES:

1.3.1 Authorization and/or Supervision (A)

Only those Workforce members who require access to ePHI to perform appropriate activities on behalf of the Plan will be permitted to have access to such information.

The HIPAA Security Officer or HIPAA Security Officer's designee will determine which Individuals or classes of individuals can access PHI and ePHI as part of their job functions, and identify the categories of PHI and ePHI to which these access rights apply. The HIPAA Security Officer or HIPAA Security Officer's designee will review requests for non-Routine Disclosures on an individual basis, using set criteria.

The Plan maintains a listing of personnel who are authorized to access PHI and ePHI. The HIPAA Privacy Officer maintains a current listing of the Covered Entity Workforce (the HIPAA "firewall").

The need for a screening process will be based on an assessment of risk, cost, benefit, and feasibility as well as other protective measures in place. Effective screening processes will be applied to allow a range of implementation, from minimal procedures to more stringent procedures commensurate with the sensitivity of the data to be accessed and the magnitude of harm or loss that could be caused by the individual.

Workforce members who work with ePHI or in areas where it may reasonably be anticipated to be accessed will be appropriately trained and supervised. Non-Workforce members and others who work in areas where ePHI may be inadvertently or incidentally viewed or accessed will receive appropriate Training and instruction regarding such information.

Please refer to the section titled "*Uses and Disclosures of Protected Health Information, For Which An Authorization Is Required*" of the Privacy Document.

The Plan has determined that current corporate-wide policies and practices are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

1.3.2 Workforce Clearance Procedures (A)

The Plan performs Workforce clearance procedures by implementing documented recruiting and hiring policies, procedures and practices on a corporate wide basis.

The Plan has determined that current corporate-wide policies and practices are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

1.3.3 Termination Procedures (A)

Upon termination of employment, access privileges to ePHI, the Plan's Information Systems and work areas where ePHI may reasonably be anticipated to be accessed will be terminated. Termination of privileges and access will be effected immediately upon the day of the termination of employment.

When access to ePHI is no longer needed for a Workforce member to perform the member's job, access privileges will be revoked or modified within 24 hours of the revocation or modification occurring, and a termination checklist is completed for these members. The listing of functions authorized to access PHI and ePHI (maintained by the HIPAA Privacy Officer) will be updated to reflect this change, if necessary. Vendors will be informed that the Workforce member's access privileges have been revoked.

The Plan has determined that current corporate-wide policies and practices are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

TOPIC: Information Access Management
SUBJECT: Ensuring that access to ePHI is authorized, established, maintained and modified based on the minimum amount necessary for a Workforce member to perform the member's job effectively.

EFFECTIVE DATE: April 20, 2005
REVISION DATES: October 1, 2017

POLICY STATEMENT:

The Plan's policies and procedures only allow for and authorize access to ePHI in a manner that is consistent with the requirements of the HIPAA Privacy Rule. Access to ePHI is therefore authorized, established, maintained and modified based on the minimum amount of information necessary for a Workforce member to perform the member's job effectively. These policies will include addressing the following HIPAA Implementation Specifications:

1.4.1 Access Authorization (A) – policies and procedures for granting access to ePHI.
1.4.2 Access Establishment and Modification (A) – policies and procedures, that based on the Plan's Access Authorization policies, establish, document, review, and/or modify a User's right of access to a Workstation, Transaction, program or process.

The Plan also specifically incorporates herein by reference those policies and procedures contained in the IT Security Policy, together with any amendments or revisions thereto.

PROCEDURES:

1.4.1 Access Authorization (A)

Access to ePHI is granted in a manner that is consistent with the Plan's determination of the minimum amount of information required by a member of the Workforce to perform the member's job. The Plan's policy on the Minimum Use of PHI (and ePHI) is documented in the Section titled "*Uses and Disclosures of Protected Health Information, Minimum Necessary Standard*" of the Privacy Document. This includes procedures and standard protocols to limit the Use and Disclosure of PHI/ePHI to the minimum information reasonably necessary to achieve the purpose of that type of Use or Disclosure.

Manager or Supervisor will authorize access to certain software and systems based on the Workforce member's job function. Access is authorized via approval workflows based on the Workforce member's job function.

The Plan has determined that current corporate-wide policies and procedures are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

1.4.2 Access Establishment and Modification (A)

The Plan maintains documentation regarding authorized access privileges. Access is modified or revoked when a User's job function or access needs change. Reviews of access rights are conducted at regular intervals to ensure continued appropriateness of levels of access.

Access privileges are revoked when a User is no longer employed by the Employer or whose job function no longer includes duties associated with the Plan. Special care is taken in deactivating access when employment is terminated, as described under the Terminations Procedures policy (See Section 1.3.3 of this Security Document).

The Plan has determined that current corporate-wide policies and procedures are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

TOPIC: Security Awareness and Training
SUBJECT: Security awareness and Training for members of the Workforce.

EFFECTIVE DATE: April 20, 2005
REVISION DATES: October 1, 2017

POLICY STATEMENT:

The Plan has implemented a Security awareness and training program for all members of its Workforce. Training on the Plan's HIPAA policies and procedures will be conducted in an appropriate manner so as to enable the members of the Workforce to carry out their job function(s) within the Plan.

Training will be provided to each appropriate member of the Workforce on Privacy, Confidentiality and Security requirements that are applicable to their work. Each new member of the Workforce will receive the Training within a reasonable period of time after joining the Plan's Workforce.

When there is a material change in the privacy policies and/or procedures, each member of the Workforce whose function is affected by the change will be trained within a reasonable period of time after the change becomes effective.

These policies will include addressing the following HIPAA Implementation Specifications:

1.5.1 Security Reminders (A) – periodic Security updates will be implemented by the Information Technology Group.
1.5.2 Protection from Malicious Software (A) – procedures for guarding against, detecting, and reporting Malicious Software will be implemented by the Information Technology Group.
1.5.3 Password Management (A) – procedures for creating, changing and safeguarding Passwords will be implemented by the Information Technology Group.

The Plan also specifically incorporates herein by reference those policies and procedures contained in the IT Security Policy, together with any amendments or revisions thereto.

PROCEDURES:

A formal Security Training program will be provided for all existing and new members of the Workforce regarding the Security and privacy of ePHI and the Plan's Information Systems. The HIPAA Security Officer or designee will determine the method of Training and documented orientation program to train appropriate staff. This may include memos, e-mailed notices, self-learning packets, distribution of policies and procedures, presentation materials, or other methods. The information can be taught at departmental meetings, training meetings, one-on-one training or by self-teaching using the methods listed. The person responsible for the training session will provide a listing of who has received the training, the trainer, and date of training and copies of information disseminated to the HIPAA Security Officer or designee.

Prior to the compliance deadline for privacy in 2003 and security in 2006, training was conducted via the delivery and review of material provided to all Plan employees in scope of this document. (See also the Section titled "*Safeguards, Privacy Training*" in the Privacy Document). A training program will be delivered to such employees via facilitated sessions, recorded sessions or online through learning development software in accordance with future deadlines.

On-going training will be conducted periodically, or within a reasonable time whenever there is a material change to the HIPAA Security requirements or to the Plan's policies and procedures. The delivery method for such on-going training may vary and/or be revised as the circumstances allow. New employees entering into roles/functions within the scope of this document will be logged in and trained within a reasonable period of time from the date they begin working with ePHI or PHI as part of their designated job function.

Training was provided to select Workforce members on the changes to the Plan's HIPAA policies and procedures, generally revised and effective as of September 23, 2013, based on changes to the HIPAA Rules, including those for Breach notification for Unsecured PHI.

The Plan will document its training in written or electronic form and maintain such documentation for at least six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

1.5.1 Security Reminders (A)

Security reminders will be sent out periodically to members of the Workforce, including management, to promote and raise awareness of Security issues, both in general and as those concerns relate to ePHI.

The Information Technology Group installs security patches and updates for computer operating systems and software to reduce known vulnerabilities as circumstances warrant.

Members of the Workforce receive periodic security reminders regarding their responsibilities with respect to guarding against, detecting and reporting malicious software from the Information Technology Group.

The Plan has determined that current corporate-wide policies and practices are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

1.5.2 Protection from Malicious Software (A)

The Information Technology Group has systems and processes in place for guarding against, detecting and reporting malicious software.

All desktops, laptops and servers associated with Workforce members and ePHI include anti-virus software with current virus definition files installed and programmed to conduct automatic virus scanning. Security updates and patches for computer operating systems and software are installed as needed to reduce known vulnerabilities.

When a significant security incident is suspected or detected that affect systems that contain ePHI, the HIPAA Security Officer or designee will be notified as soon as possible. Workforce members are not allowed to proceed with virus eradication efforts without appropriate

authorization and/or supervision from the Information Technology Group. The infected machine, along with any other machines that may have been contaminated must be isolated from the network, scanned and repaired by the appropriate technology support personnel.

Workforce members are instructed not to download software from the Internet or install software on desktops or laptops without prior authorization.

Workforce members are instructed not to open e-mail attachments from unknown or untrustworthy sources. All e-mail attachments are scanned for the presence of viruses.

The Plan has determined that current corporate-wide policies and practices are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

1.5.3 Log-in Monitoring (A)

The Information Technology Group is responsible for monitoring and reporting production, network and security systems (Security Events) in a System Log.

The Systems Log will be retained according to the Plan's record retention guidelines.

The Plan has determined that current corporate-wide policies and practices are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

1.5.4 Password Management (A)

The Information Technology Group is responsible for establishing guidelines for creating, changing and safeguarding Passwords.

The Plan has determined that current corporate-wide policies and practices are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

TOPIC: Security Incident Procedures
SUBJECT: Policies and procedures to address Security Incidents.

EFFECTIVE DATE: April 20, 2005
REVISION DATES: October 1, 2017

POLICY STATEMENT:

The Plan maintains policies and procedures which are reasonably designed to address and identify all Security Incidents, including the attempted or successful unauthorized access, Use, Disclosure, modification, or destruction of information or interference with systems operations in an Information System. These policies will include the following HIPAA Implementation Specification:

1.6.1 Response and Reporting – The Information Technology Group will identify and respond to suspected or known Security Incidents; mitigate, to the extent practicable, harmful effects of known Security Incidents; and document Security Incidents and their outcomes.

The Plan also specifically incorporates herein by reference those policies and procedures contained in the IT Security Policy, together with any amendments or revisions thereto.

PROCEDURES:

1.6.1 Response and Reporting

Plan Workforce members are trained to report suspected or actual Security Incidents dealing with unauthorized access, Use, Disclosure, modification, or destruction of ePHI to the HIPAA Security Officer as soon as practicable. This includes incidents such as denial of service attacks, malicious code, viruses and worms.

All known Security Incidents will be investigated and documented. An appropriate response to a Security Incident will be determined based on the nature and severity of the Security Incident. Responses may include, but are not be limited to:

(a) the application of Sanctions against responsible personnel;
(b) the initiation of (additional) Security reminders;
(c) additional and/or updated Training on Security practices; and
(d) an evaluation of the adequacy of the Plan's existing Security Measures.

Any harm resulting from a Security Incident will be mitigated to the extent practicable.

All known Security Incidents, together with the results of associated investigations will be documented and the results maintained according to the Plan's record retention guidelines. Security Incidents involving an improper Disclosure of ePHI will be logged and maintained in conjunction with the Section titled "*Participants' Rights, Right to Receive an Accounting of Disclosures*" in the Privacy Document for a period to comply with the corporate-wide records retention policy.

TOPIC: Contingency Plan
SUBJECT: Policies and Procedures for Responding to Systems Emergencies.

EFFECTIVE DATE: April 20, 2005
REVISION DATES: October 1, 2017

POLICY STATEMENT:

The Plan will establish, and implement as necessary, policies and procedures for responding to emergencies and other occurrences (for example, fire, vandalism, system failure, and natural disaster) that damage systems containing ePHI. Such policies and/or business continuity plans are required for all critical business functions of the Plan. These policies will establish the elements involved with business resumption in the event of a disaster and will include the following HIPAA Implementation Specifications:

1.7.1 Data Backup Plan – The Information Technology Group will establish and implement procedures to create and maintain exact, retrievable copies of ePHI.
1.7.2 Disaster Recovery Plan – The Information Technology Group will establish procedures to restore any loss of data will be established.
1.7.3 Emergency Mode Operation Plan – The Information Technology Group will establish (and implement as needed) procedures to enable continuation of critical business processes for the protection of the Security of ePHI while operating in emergency mode.
1.7.4 Testing and Revision Procedures (A) – The Information Technology Group will establish procedures for periodic testing and revision of contingency plans.
1.7.5 Applications and Data Criticality Analysis (A) – The Plan will assess the relative criticality of specific applications and data in support of other contingency plan components will be assessed.

The HIPAA Security Officer or designee will provide support and direction for the implementation of the contingency plan as it may relate to ePHI.

The Plan also specifically incorporates herein by reference those policies and procedures contained in the IT Security Policy, together with any amendments or revisions thereto.

PROCEDURES:

1.7.1 Data Backup Plan

The Information Technology Group will establish appropriate controls and procedures for retrieving copies of ePHI by:

(a) Identifying systems that contain ePHI and verifying these systems are covered by the Employer's backup policy;
(b) Clearly labeling backup media;
(c) Documenting the rotation cycle and offsite storage for backup media;
(d) Recording backups on logs to provide an audit trail of backup history; and
(e) Restoring testing to verify the integrity of backup media.

The Employer will review the backup policy periodically for any necessary changes.

1.7.2 Disaster Recovery Plan

IT Systems Disaster Recovery Standard has been established to allow for the restoration of any loss of data and/or ePHI.

The Disaster Recovery Plan will be sent to a designated repository so that it will be accessible to the team implementing the Disaster Recovery Plan in the event of a disruption to normal system processing capabilities.

1.7.3 Emergency Mode Operation Plan

The Plan maintains procedures to allow the continuation of the Plan's critical business processes and to protect ePHI while operating in emergency mode.

Temporary access to ePHI within the Plan's information system is provided in emergencies through the Employer's Business Continuity plan.

Some backup of ePHI is provided by the Plan's vendors in case of emergencies.

The Plan's contingency plan is described the Plan's emergency access procedures.

1.7.4 Testing and Revision Procedures (A)

The Plan maintains procedures to allow the continuation of the Plan's critical business processes and to protect ePHI while operating in emergency mode.

The Plan has determined that current corporate-wide policies and procedures are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

1.7.5 Applications and Data Criticality Analysis (A)

The relative criticality of the Plan's applications and data are periodically reviewed by the Plan in conjunction with the assessment of other contingency plan components.

The Plan determines and documents the systems that contain ePHI.

The Plan establishes an order or priority for protecting the integrity and security of participant data.

The Employer has established the IT Systems Disaster Recovery Standard, back-up plan and offsite storage system to protect all information, including ePHI. The Information Technology Group assesses whether or not the plan or software is critical to maintain normal operations and whether it is critical to the overall contingency plans.

The Employer's ePHI resides in systems that are covered by the corporate business continuity plan. Because the Employer's ePHI is not business critical, nor is it critical to the continuation of the Plan, no further disaster recovery plan is required.

The Plan has determined that current corporate-wide policies and practices are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

TOPIC: Facility Access Controls
SUBJECT: Limiting physical access to the Plan's electronic Information Systems and Facilities.

EFFECTIVE DATE: April 20, 2005
REVISION DATES: October 1, 2017

POLICY STATEMENT:

The Plan has implemented and maintains policies and procedures regarding Facility access controls to limit physical access to the company's Facilities, work areas and electronic Information Systems, while ensuring that properly authorized access is allowed. These policies will include addressing the following HIPAA Implementation Specifications:

2.1.1 Contingency Operations (A) – The Facilities Group will establish and implement as necessary procedures to allow Facility access in support of restoration of lost data under the disaster recovery plan and emergency operation plan in the event of an emergency

2.1.2 Facility Security Plan (A) – The Facilities Group will implement policies and procedures to safeguard the Facility and the equipment therein from unauthorized physical access, tampering and theft.

2.1.3 Access Control and Validation Procedures (A) – The Facilities Group will implement procedures to control and validate a person's access to Facilities based upon their role or function, including visitor control, and control of access to software programs for testing.

2.1.4 Maintenance Records (A) – The Facilities Group will implement policies and procedures to document repairs and modifications to the physical components of a Facility which are related to Security (for example, hardware, walls, doors and locks).

The Plan also specifically incorporates herein by reference those policies and procedures contained in the IT Security Policy, together with any amendments or revisions thereto.

PROCEDURES:

2.1.1 Contingency Operations (A)

The Plan's contingency plan in accordance with Section 164.308(a)(7) describes the Plan's emergency access procedures. The Employer's continuity of IT Systems and computing environment is governed by the IT Systems Disaster Recovery Standard. Additionally, business users have business continuity planning in place for dealing with emergency incidents.

The Plan has determined that current corporate-wide policies and practices are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

2.1.2 Facility Security Plan (A)

Department managers or team leaders supervise all Workforce members who work with ePHI or in areas where it may be accessed.

Non-Workforce members, including maintenance personnel or software vendors, who work with ePHI or in areas where it may be accessed, must receive appropriate authorizations from the HIPAA Security Officer or designee and be supervised while on-site.

The Employer maintains a Facility Security Plan to document physical security measures intended to prevent unauthorized access to the Company's and Plan's facility and tampering or theft of its equipment.

To ensure that only authorized individuals have access to the Plan's work area and electronic information systems, access is controlled and validated through locks or key card access to the facility in general with additional locks or key card restrictions for access to the Plan's work areas.

Oxy employees are issued access badges that grants them general access to Oxy common work areas. Each departmental area is considered restricted space and prior approval from Oxy management and security is required to access restricted areas. The same process applies for granting access to secured areas that are repositories of confidential information such as personnel archives, legal files, company sensitive records, etc.

If an employee misplaces and/or loses his/her access badge, he/she needs to report it immediately to security so it can be deactivated. If applicable, a temporary access badge will be issued after the affected employee presents a valid form of identification such as a driver's license, passport, military photo card, etc. A replacement access badge will be issued after processing.

Visitors to each facility are required to check in with building security and obtain a security badge. After identity verification is completed, security will then notify the host employee that his/her visitor is waiting to be escorted. All visitors must be escorted by host employee at all times. Visitors are required to check out with security prior to their departure.

Oxy employees visiting from other Oxy locations must conform to this same visitor protocol to validate their identity and active employee status.

Contractors and vendors must be pre-authorized for any work and/or services being performed. Contractor and/or vendor personnel must provide valid form of identification such as driver's license, passport, military photo card, etc. to verify their identity. In some instances and if applicable and at the request of the Facilities Group, temporary access during non-business hours may be granted to restricted areas to complete requested work.

Visitors to the Facilities must be escorted as appropriate and, if working near or with ePHI, have appropriate authorization and/or supervision.

Temporary authorization to access the Plan's facility and electronic information systems is granted to repair personnel or technicians during emergencies for the purposes of restoring lost data or repairing damaged equipment.

Members of the Plan's Workforce are restricted from accessing ePHI during emergencies until data is restored and/or damaged equipment is repaired.

The Plan has determined that current corporate-wide policies and practices are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

2.1.3 Access Control and Validation Procedures (A)

Documentation is maintained for all keys, key cards and physical access controls.

Access privileges are modified or revoked whenever a Workforce member's job function or access needs change. Modifications or revocations to physical access are made with appropriate authorization.

A termination checklist is completed for Workforce members for whom continued physical access is no longer warranted.

The Plan has determined that current corporate-wide policies and practices are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

2.1.4 Maintenance Records (A)

To ensure that only authorized Individuals have access to the Plan's work and electronic information systems, access is controlled and validated through locks or key card access to the facility in general with additional locks or key card restrictions for access to the Plan's work areas.

The Plan has determined that current corporate-wide policies and practices are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

The Facilities Group maintains any repairs or modifications related to security.

TOPIC: Workstation Use
SUBJECT: Specifying the proper functions, manner of use and physical attributes of Workstations.

EFFECTIVE DATE: April 20, 2005
REVISION DATES: October 1, 2017

POLICY STATEMENT:

The Plan has implemented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical surroundings of a specific workstation or class of workstations that can access ePHI. The Plan also specifically incorporates herein by reference those policies and procedures contained in the IT Security Policy, together with any amendments or revisions thereto.

Workstation means 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.

Workstations that contain or have access to ePHI are used and physically safeguarded in a manner that maximizes security and prevents unauthorized access.

PROCEDURES:

Workforce members utilize the Employer-owned and maintained workstations in the course of normal business on behalf of the Plan. The functions that can be performed by Workforce members is determined by their role and based upon approved and authorized User access requests. Workstations are configured with the appropriate software and applications based upon these approved functions.

Workstations and display screens should be positioned in such a manner that any ePHI displayed is not easily viewable by others. When display screens are located in cubicles or open areas within a Facility, privacy screens should be used to reduce or eliminate the possibility of peripheral viewing.

Training is provided to members of the Workforce regarding acceptable uses of workstations that contain or permit access to ePHI are provided to members of the Workforce. Additional Training may be provided on an as needed basis to ensure Workforce members understand procedures for compliance.

TOPIC: Workstation Security
SUBJECT: Physical safeguards for all Workstations with access to ePHI to restrict access to authorized Users.

EFFECTIVE DATE: April 20, 2005
REVISION DATES: October 1, 2017

POLICY STATEMENT:

Oxy will implement Physical Safeguards for Workstations that access ePHI in order to restrict access to authorized Users.

Workstation means 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.

PROCEDURES:

The Plan has taken reasonable precautions to confirm that such workstations are physically safeguarded in a manner that maximizes Security and prevents unauthorized access.

Workforce members are required to take reasonable steps to prevent unauthorized access of unattended workstations, limit the ability of unauthorized persons to view sensitive information, and erase sensitive information as needed.

Additional care must be given to safeguarding portable electronic computing devices, such as laptops, Personal Digital Assistants (PDAs), smart phones, tablets and wireless e-mail devices. This additional level of care applies whether the portable device is located within or outside of the Plan's Facility. Portable devices must not be left unsecured and unattended. Secure locking devices may be used to secure portable devices to the Workforce member's desk or workspace.

Any loss or theft of a portable electronic device containing ePHI must be reported immediately to the HIPAA Security Officer or designee. Mitigation procedures such as those contained in the Section titled "*Safeguards, Mitigation*" of the Privacy Document must be implemented promptly.

Members of the Workforce using laptops or remote dial-in systems should be discouraged from downloading ePHI onto laptops or remote systems. Workforce members must use reasonable caution when accessing ePHI from remote locations or from any system outside of that Workforce member's secure work area. Workstations and display screens should be positioned in such a manner that any ePHI displayed is not easily viewable to others. When display screens are located in cubicles or open areas within a facility, privacy screens should be used to reduce or eliminate the possibility of peripheral viewing.

Training is provided to members of the Workforce regarding acceptable uses of Workstations that contain or permit access to ePHI. Additional training may be provided on an as needed basis to ensure Workforce members understand all procedures for compliance.

TOPIC: Device and Media Controls
SUBJECT: Management of the receipt, removal and movement of hardware and Electronic Media that contain ePHI.

EFFECTIVE DATE: April 20, 2005
REVISION DATES: October 1, 2017

POLICY STATEMENT:

With respect to Company owned or leased devices or devices that the Company supports, the Plan has implemented policies to govern the receipt and removal of hardware and Electronic Media that contain ePHI into and out of its Facilities, as well as the movement of these items within its Facilities. These policies will include the following HIPAA Implementation Specifications:

2.4.1 Disposal – The Information Technology Group will implement policies and procedures to address the final disposition of ePHI and/or the hardware or Electronic Media on which it is stored will be implemented. See the Employer's record retention policies maintained by the HIPAA Privacy Officer.

2.4.2 Media Re-Use – The Information Technology Group will establish procedures to remove ePHI from Electronic Media before the media are made available for reuse.

2.4.3 Accountability (A) – The Information Technology Group will maintain a record of the movements of hardware and the person responsible for that record will be maintained.

2.4.4 Data Backup and Storage (A) – The Information Technology Group will create exact, retrievable copies of ePHI (no including portable devices) when needed, prior to the movement of equipment.

The Plan also specifically incorporates herein by reference those policies and procedures contained in the IT Security Policy, IT-ITS-ST-99-0216 Standard for Smart Device Use, IT-ITS-PR-0197 IT Hardware Asset Disposal Procedure, IT-ITS-ST-99-0128 Standard for IT Hardware Asset Management and IT-ICS-ST-90-0115 IT Business Continuity Plan together with any amendments or revisions thereto.

PROCEDURES:

Within the Plan, ePHI may be stored or maintained on hardware and Electronic Media such as storage devices (servers and hard disk drives), workstations, laptops, diskettes, CDs, and other portable devices used to access e-mail (*e.g.*, iPhones or PDAs).

2.4.1 Disposal

Please refer to the Data retention policy and the IT Hardware Asset Disposal Procedure.

2.4.2 Media Reuse

An accurate inventory of the Plan's hardware and electronic media is maintained and updated as needed.

ePHI is stored on the hard drives of computers or other electronic media is removed before the disposal or re-use of the hardware or electronic media.

The effective removal of ePHI from hardware or electronic media is verified prior to disposal or allowing re-use.

2.4.3 Accountability (A)

An accurate inventory of the Plan's hardware and electronic media is maintained and updated as needed.

The Plan has determined that current corporate-wide policies and practices are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

2.4.4 Data Backup and Storage (A)

When needed an exact and retrievable copy of ePHI not on portable devices is created before activities that may result in damage or the loss of data.

This process is completed in accordance with the Data Backup Plan as required by Section 164.308(a)(7)(ii)(A).

The Plan has determined that current corporate-wide policies and practices are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

TOPIC: Access Control
SUBJECT: Technical Security measures for the Plan's electronic Information Systems.

EFFECTIVE DATE: April 20, 2005
REVISION DATE: October 1, 2017

POLICY STATEMENT:

Technical Security measures, policies and procedures have been implemented for electronic Information Systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights. These policies will include the following HIPAA Implementation Specifications:

- 3.1.1 Unique User Identification – The Information Technology Group will assign a unique name and/or number for identifying and tracking User identity.
- 3.1.2 Emergency Access Procedure – The Information Technology Group will establish and implement procedures for obtaining necessary ePHI during an emergency.
- 3.1.3 Automatic Logoff (A) – The Information Technology Group will implement electronic procedures that terminate an electronic application session after a predetermined period of inactivity.
- 3.1.4 Encryption and Decryption (A) – The Information Technology Group will implement a mechanism to encrypt and decrypt ePHI while in transit.

The Plan also specifically incorporates herein by reference those policies and procedures contained in the IT Security Policy, together with any amendments or revisions thereto.

PROCEDURES:

3.1.1 Unique User Identification

Workforce members are assigned unique User Identification names or numbers that enable the Information Technology Group to identify, authenticate and track User identity.

User accounts are established that are consistent with administrative policies and procedures that authorize and grant access privileges.

Access control lists are maintained and updated as needed and technical modifications to user accounts are provided in a timely manner when access privileges are terminated or changed.

3.1.2 Emergency Access Procedure

Temporary access to the Plan's Information Systems and/or ePHI is provided in the event of emergencies. The Plan's contingency plan (see also the policies and procedures set forth under Contingency Plan standard in section 1.7) sets forth the Plan's emergency access procedures.

The Employer's ePHI is not considered business critical. Data that is critical to the continuation of the Plan is housed at vendor sites. Should a need arise to access ePHI during an emergency, the vendors will be contacted.

3.1.3 Automatic Logoff (A)

A Password protected screen saver is implemented after 30 minutes inactivity.

The Plan has determined that current corporate-wide policies and practices are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

3.1.4 Encryption and Decryption (A)

The Plan has determined that Encryption and decryption generally are not required for the electronic maintenance of ePHI as it may be used by the Plan in its day-to-day activities. Access to such ePHI is restricted to those Workforce members who require it to perform their job functions. Workforce members may also protect ePHI with password-protection or through the use of ZixMail or via secured system sponsored by the Plan's vendors. Numerous other safeguards are also in place to protect ePHI as described in this Security Document.

At the present time, due to the limited risk of inappropriate Use or Disclosure of ePHI and the limited technological capability of the Plan to encrypt and decrypt ePHI in storage for its operating systems and storage platforms, the Plan has determined that its policy will not be to encrypt ePHI at rest. The alternate controls described in this Security Document have been determined to be reasonable and appropriate to mitigate the risk to ePHI.

The HIPAA Security Officer may nevertheless authorize or mandate the use of Encryption and decryption on an as needed basis as may be appropriate given the nature of the information stored and the potential risks posed.

The Plan has determined that current corporate-wide policies and practices are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

TOPIC: Audit Controls
SUBJECT: Recording and examining activity in Information Systems that contain or use ePHI.

EFFECTIVE DATE: April 20, 2005
REVISION DATE: October 1, 2017

POLICY STATEMENT:

The Information Technology Group will implement hardware, software, and/or procedural mechanisms that record and examine activity in Information Systems that contain or use ePHI.

PROCEDURES:

The Employer has determined that it is not reasonable or appropriate to implement this policy.

TOPIC: Integrity
SUBJECT: Protecting ePHI from improper alteration or destruction.

EFFECTIVE DATE: April 20, 2005
REVISION DATE: October 1, 2017

POLICY STATEMENT:

All ePHI maintained in the Plan's Information Systems is protected from improper alteration or destruction. The Plan has considered the risk and potential for improper alteration or destruction of ePHI maintained in its systems and has determined that the policies and procedures set forth herein are reasonable and sufficient to ensure the Integrity of the ePHI.

PROCEDURES:

The Employer has determined that it is not reasonable or appropriate to implement this policy.

TOPIC: Person or Entity Authentication
SUBJECT: Verifying that a person or entity seeking access to ePHI is the one claimed.

EFFECTIVE DATE: April 20, 2005
REVISION DATE: October 1, 2017

POLICY STATEMENT:

The Plan has implemented reasonable procedures to verify that a person or entity seeking access to ePHI is the one claimed.

PROCEDURES:

Note: All employees of the Employer are assumed to be "known" by the Workforce for the purposes of this policy.

When responding to a request for ePHI, the authorized Workforce member will take steps to ensure that the person is actually who they say they are and has authorization to receive or access the ePHI, if not a key contact or known by the Workforce.

The authorized Workforce member shall request information sufficient to verify that person's identity and affiliation if not a key contact or known by the Workforce.

If an authorized Workforce member is unable to verify the identity of the person, no ePHI will be transmitted in any form to the requesting party if not a key contact or known by the Workforce.

Additional specific authentication procedures are described below.

3.4.1 Authenticate E-mail – An authorized Workforce member who transmits mail electronically must take reasonable steps to verify that each intended recipient is a person to whom the authorized Workforce member is required, permitted, or authorized to disclose PHI, as described in this Policy. The authorized Workforce member must take reasonable steps to verify that outgoing e-mail is addressed only to a person(s) to whom the authorized Workforce member is required, permitted, or authorized to disclose PHI as described in this Policy. Thus, on outgoing e-mail correspondence containing PHI, the authorized Workforce member may not routinely copy other persons to whom an Individual directed his or her correspondence (whether as "cc" or directly). Instead, the authorized Workforce member first must consider whether the persons copied on the original correspondence are authorized to receive the PHI.

The authorized Workforce member must advise third parties to send e-mail containing PHI to a business e-mail account accessible only by the authorized Workforce member (and such other employees with a legitimate need to use or access such PHI in the performance of Health Plan functions).

3.4.2 Authenticate Telephonic and Other Verbal Communication of PHI – The authorized Workforce member must take reasonable steps to ensure that telephone and other verbal conversations in which PHI is discussed are not overheard by persons who do not have a legitimate need to know the content of the conversation. For example, conferences in which PHI is discussed generally should be conducted in a closed room or in a low tone of voice unlikely to be overheard.

Before engaging in a conversation in which the authorized Workforce member may disclose PHI, the authorized Workforce member must take reasonable steps to verify that the other party (or parties) is a person (or persons) to whom the authorized Workforce member is required, permitted, or authorized to disclose PHI, as described in this Policy.

3.4.3 Authenticate Recorded Messages– An authorized Workforce member who leaves a recorded message containing PHI must take reasonable steps to verify that each intended recipient is a person to whom the authorized Workforce member is required, permitted or authorized to disclose PHI, as described in this Policy. An authorized Workforce member may leave a recorded message containing an Individual's PHI on an Individual's home answering machine or voicemail account only if (a) the answering machine or voicemail message indicates that it is the answering machine or voicemail account for the Individual (or his or her residence), and (b) the Individual has instructed the authorized Workforce member to leave the message.

TOPIC: Transmission Security
SUBJECT: Technical Security measures to guard against unauthorized access to ePHI that is transmitted over an electronic communications network.

EFFECTIVE DATE: April 20, 2005
REVISION DATE: October 1, 2017

POLICY STATEMENT:

The Plan has implemented technical Security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. These policies will include addressing the following HIPAA Implementation Specifications:

3.5.1 Encryption (A) – The Information Technology Group will implement mechanisms to encrypt ePHI whenever deemed appropriate.

The Plan also specifically incorporates herein by reference those policies and procedures contained in the IT Security Policy, together with any amendments or revisions thereto.

PROCEDURES:

ePHI has been classified by the Plan as high risk information and should not be transmitted electronically unless reasonable methods have been taken to protect its Security. Only authorized Individuals may transmit ePHI. If ePHI is transmitted via e-mail communications, only the minimum amount of PHI needed to achieve the purpose of the communication is allowed to be transmitted. This should be determined in accordance with the Plan's Minimum Use of PHI policy contained in the Section titled "*Uses and Disclosures of Protected Health Information, Minimum Necessary Standard*" of the Privacy Document.

When transmitting PHI via e-mail communications, the following Statement (or its equivalent) should be included:

THIS ELECTRONIC MESSAGE TRANSMISSION, INCLUDING ANY ATTACHMENTS, CONTAINS INFORMATION AND/OR TRADE SECRETS OF OCCIDENTAL WHICH MAY BE CONFIDENTIAL OR PRIVILEGED. UNAUTHORIZED USE OR DISCLOSURE IS PROHIBITED.

The information is intended to be for the use of the individual or entity named above. If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this information is prohibited. If you have received this electronic transmission in error, please notify the sender immediately by a "reply to sender only" message and destroy all electronic and hard copies of the communication, including attachments.

3.5.1 Integrity Controls (A)

ePHI may only be transmitted to authorized parties.

When ePHI must be transmitted in email communications, only the minimum amount of ePHI needed to achieve the purpose of the communication is allowed to be transmitted and must be in accordance with the Plan's Minimum Necessary disclosure policies and procedures.

The Plan has determined that the current corporate-wide policies and practices are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

3.5.2 Encryption (A)

Although Encryption is not generally required for the electronic transmittal of ePHI that may be used by the Plan, if it is determined by the HIPAA Security Officer that Encryption is required in a given circumstance, an Encryption method will be coordinated with the recipient of e-mail communications containing PHI.

The Plan has determined that the current corporate-wide policies and practices are sufficient to meet this aspect of the Security Rule. Therefore, no additional procedures will be implemented and the Plan will rely on current practices.

TOPIC: Breach of Unsecured PHI
SUBJECT: Notification to Individuals, the media and the Secretary.

EFFECTIVE DATE: September 23, 2009
REVISION DATE: October 1, 2017

POLICY STATEMENT:

The Plan has established policies and procedures to provide notification following the discovery of a Breach of Unsecured PHI to, as applicable, affected Individuals, the media and the Secretary.

Notification to Individuals. The Plan will, following the discovery of a Breach, notify each Individual whose Unsecured PHI has been, or is reasonably believed by the Plan to have been accessed, acquired, used or disclosed as a result of such Breach.

Notification to the Media. For a breach of Unsecured PHI involving more than 500 residents of a State or jurisdiction, the Plan will, following discovery of the Breach, notify prominent media outlets serving the State or jurisdiction.

Notification to the Secretary. The Plan will, following the discovery of a Breach of Unsecured PHI, notify the Secretary.

Discovery of Breach. A Breach will be treated as discovered by the Plan as of the first day on which such Breach is known to the Plan, or, by exercising reasonable diligence would have been known to the Plan. The Plan will be deemed to have knowledge of a Breach if such Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is a Workforce member or agent of the Plan (determined in accordance with the federal common law of agency).

Risk Assessment. Following discovery of a potential Breach, the Plan will begin an investigation, conduct a risk assessment and, based on the results of the risk assessment, begin the applicable notification process.

Administrative Requirements. The Plan will comply with the administrative requirements applicable to this policy for Breach of Unsecured PHI with respect to: Training, Individuals' complaints to the Plan, Sanctions against Workforce members who fail to comply with the Plan's Breach of Unsecured PHI policies, refraining from intimidating or retaliatory acts, waiver of rights implementation of policies and procedures, and changes to the Plan's policies and procedures.

PROCEDURES:

Breach Investigation

The HIPAA Privacy Officer or his designee will act as the investigator of the Breach. The investigator will be responsible for the management of the Breach investigation, completion of a risk assessment, and coordinating with others, as appropriate. All documentation related to the Breach investigation will be retained for a minimum of six (6) years.

Risk Assessment

To determine if an impermissible use or disclosure of PHI constitutes a Breach and requires notification to an affected Individual or the Secretary, the Plan will perform a risk assessment. This risk assessment will be performed jointly by the HIPAA Privacy Officer or his designee and the Employer's employee benefits counsel. A breach is presumed to have occurred unless the covered entity or a business associate can demonstrate that there is a low probability that the PHI has been compromised. A breach notification is not required if a Covered Entity and Business Associate can demonstrate through a risk assessment that a low probability exits that the PHI has been compromised. The Plan will document the risk assessment noting the outcome of the risk assessment process. In performing the risk assessment, the assessment will be fact specific and the Plan will consider a number of or combination of factors, such as: (1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (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.

Notification

Notification to Individuals.
The Plan will provide the notification to an Individual whose Unsecured PHI has been the subject of a Breach without unreasonable delay and in no case later than sixty (60) days after discovery of a Breach.

Content of Notification. The notification will include, to the extent possible:

a. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;
b. 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);
c. Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;
d. 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

e. Contact procedures for Individuals to ask questions or learn additional information, which will include a toll-free telephone, an email address, Web site, or postal address.

The notification will be written in plain language.

Method of Notification. The notification will be provided in one of the following forms, based on the appropriateness for the situation:

Written notice. The Plan will provide written notification by first-class mail to the Individual at the last known address of the Individual or, if the Individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available. If the Plan knows the Individual is deceased and has the address of the next of kin or personal representative of the Individual, the Plan will provide the written notification by first-class mail to either the next of kin or personal representative of the Individual. The notification may be provided in one or more mailings as information is available. The Company may also provide companywide communication via email or on the Company's intranet in addition to written notice describing the event and the Company's subsequent action on behalf of the Plan.

Substitute notice. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the Individual as described above, a substitute form of notice reasonably calculated to reach the Individual will be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the Individual.

- In the case in which there is insufficient or out-of-date contact information for fewer than ten (10) Individuals, then such 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 ten (10) or more Individuals, then such substitute notice will:
    - Be in the form of either a conspicuous posting for a period of ninety (90) days on the Company intranet site for employee matters, 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 ninety (90) days where an Individual can learn whether the Individual's Unsecured PHI may be included in the Breach.

Additional Notice in Urgent Situations. In any case deemed by the Plan to require urgency because of possible imminent misuse of Unsecured PHI, the Plan may provide information to Individuals by telephone or other means, as appropriate, in addition to the notices described above.

Notification to the Media.

For a Breach of Unsecured PHI involving more than 500 residents of a State or jurisdiction, the Plan will, upon discovery of the Breach, notify prominent media outlets serving the State or jurisdiction. The Plan will provide the notification without unreasonable delay and in no case later than sixty (60) days after discovery of the Breach. The content of the notification to the media will meet the requirements described above for Notification to Individuals. The media is not required to print or run information about the breach.

Notification to the Secretary.
The HIPAA Privacy Officer on behalf of the Plan will, following the discovery of a Breach of Unsecured PHI, notify the Secretary. For Breaches of Unsecured PHI involving 500 or more Individuals, the HIPAA Privacy Officer and the Employer's employee benefits counsel will, subject to the exception noted below, provide this notification contemporaneously with the notice required to Individuals on behalf of the Plan and in the manner specified on the HHS Web site at:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

Exception. If a Law Enforcement Official states to the Plan that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the Plan will: (a) if the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) 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 and no longer than thirty (30) days from the date of the oral statement, unless a written statement is submitted during that time.

Maintenance of Breach Log

For Breaches of Unsecured PHI involving less than 500 Individuals, the Plan will maintain a log or other documentation of such Breaches and, not later than sixty (60) days after the end of each calendar year, provide this notification for Breaches occurring during the preceding calendar year, in the manner specified on the HHS Web Site.

The Plan will maintain a process to record or log all breaches of Unsecured PHI. The following information will be logged for each Breach:

(1) A description of what happened, including the date of the Breach, the date of the discovery of the Breach, and the number of Individuals affected, if known.

(2) A description of the types of Unsecured PHI that were involved in the Breach (e.g., full name, Social Security number, date of birth, account number, home address).

(3) A description of the action taken with regard to notification of the affected Individuals or the Secretary regarding the breach.

Administrative Requirements

The Plan will apply the same policies applicable to the Privacy Rule to this policy for Breach of Unsecured PHI with respect to: Training, Individuals' complaints to the Plan, Sanctions against Workforce members who fail to comply with the Plan's Breach of Unsecured PHI policies, refraining from intimidating or retaliatory acts, waiver of rights, implementation of policies and procedures, and changes to the Plan's policies and procedures.

This Beach Notification Log and procedures against retaliatory acts will be maintained by the HIPAA Privacy Officer for Benefits or designee and shall be available upon written request to:

Occidental Petroleum Corporation.
Attention: HIPAA Privacy Officer
5 Greenway Plaza, Suite 110
Houston, Texas 77046

APPENDIX LIST

Appendices	Topic
Appendix A	HIPAA Terms and Definitions
Appendix B	Covered Entity List
Appendix C	Business Associate Agreement Inventory
Appendix D	Form of Business Associate Contract
Appendix E	Notice of Privacy Rights and Practices
Appendix F	Complaints Log
Appendix G	Plan Document Language (see Privacy Document)
Appendix H	HIPAA Non-Routine Disclosure Log
Appendix I	Training Documentation
Appendix J	Breach Notification Log

TOPIC: Definitions of HIPAA Terms
SUBJECT: HIPAA Terms and Definitions.

EFFECTIVE DATE: April 14, 2003
REVISION DATE: October 1, 2017

Access – The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to "Access" as used in regard to the HIPAA Security Rule, but not the HIPAA Privacy Rule.)

Administrative Safeguards – Administrative actions, and the 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.

Authentication – The corroboration that a person is the one claimed.

Authorization – The mechanism for obtaining permission for the Use and/or Disclosure of Health Information at any time other than at time of enrollment.

Availability – The property that data or information is accessible and useable upon demand by an authorized person.

Breach - The acquisition, access, Use, or Disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the Security or Privacy of the PHI.

(1) Breach excludes:

- Any unintentional acquisition, access or use of PHI by a Workforce member or person acting under the authority of a Covered Entity or Business Associate if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further Use or Disclosure in a manner not permitted under the Privacy Rule.
- Any inadvertent Disclosure by a person who is authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the same Covered Entity or Business Associate, or Organized Health Care Arrangement in which the Covered Entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
- A Disclosure of PHI where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the Disclosure was made would not reasonably have been able to retain such information.

(2) Except as provided in paragraph (1) of this definition, an unauthorized acquisition, Access, Use, or Disclosure of Unsecured PHI in a manner not permitted under the Privacy Rule is presumed to be a Breach unless the Covered Entity or Business Associate, as applicable,

demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

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

Business Associate -

A(n) person/entity outside the Plan's Workforce of the Covered Entity who

- Creates, receives, maintains, or transmits PHI for a function or activity regulated under the HIPAA Privacy rule, including claim processing or administration, data analysis, processing, or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR §3.20, billing, benefit management, practice management, and repricing, or
- Provides legal, actuarial, accounting, consulting, data aggregation, (as defined in 45 CFR §164.501) management, administrative, accreditation, or financial services to or for such covered entity, or to or for an Organized Health Care Arrangement in which the Covered Entity participates, where the provision of the service involves the Disclosure of PHI from (a) the Covered Entity, (b) the Organized Health Care Arrangement, or (c) from another Business Associate of the Covered Entity or Organized Health Care Arrangement, to the person/entity.

A Covered Entity may be a Business Associate of another Covered Entity.

Business Associate includes:

- A Health Information Organization, E-prescribing Gateway or service, patient safety organization or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information
- A person that offers a personal health record to one or more Individuals on behalf of a covered entity
- A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate

Business Associate does not include:

- A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the Individual
- A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent the Security Rule permits the exclusion
- A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the

extent such activities are authorized by law

- A Covered Entity participating in an Organized Health Care Arrangement that performs a function or activity as described in this definition for or on behalf of such Organized Health Care Arrangement, or that provides a service as described in this definition to or for such Organized Health Care Arrangement by virtue of such activities or services.

Confidentiality – The property that data or information is not made available or disclosed to unauthorized persons or processes.

Covered Entity – A Health Plan, a Health Care Clearinghouse, or a Health Care Provider who transmits any Health Information in electronic form in connection with a standard or covered Transaction.

Covered Functions – Those functions of a Covered Entity the performance of which makes the entity a Health Plan, Health Care Provider, or Health Care Clearinghouse.

Designated Record Set – A group of Records maintained by or for a Group Health Plan, consisting of enrollment, Payment, claims adjudication, and case or medical management record systems; or used, in whole or in part, by or for the Covered Entity to make decisions about Individuals. Please also refer to the definition of "Record."

Digital Information Security Policy – Policy Number 16:02:00.

Disclosure – The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Electronic Media – Electronic storage media on which data is or may be recorded electronically, including, for example, memory 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 (wide-open), intranet, extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, electronically stored voice transmissions, 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, because the information being exchanged did not exist in electronic form before the Transaction.

Electronic Protected Health Information (ePHI) – Protected Health Information that is transmitted by or maintained in Electronic Media.

Encryption – The use 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, and such process or key has not been breached.

Facility – The physical premises and the interior and exterior of a building(s).

Facilities Group – The facilities management department at Houston Greenway Plaza, Oxy Permian Plaza, the Midland Technical Training or Corporate Woods Office in Tulsa, Oklahoma, as appropriate or applicable.

Family Member – With respect to an Individual, a Family Member is: (1) A dependent of the Individual; or (2) Any person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the Individual or of a dependent of the Individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).

First-degree relatives include parents, spouses, siblings, and children. Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces. Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins. Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.

Genetic Information –

(1) Subject to paragraphs (2) and (3) below, Genetic Information means, with respect to any Individual, information about: (i) Such Individual's Genetic Tests; (ii) The Genetic Tests of Family Members of such Individual; (iii) The Manifestation of a disease or disorder in Family Members of such Individual; or (iv) Any request for, or receipt of, Genetic Services, or participation in clinical research which includes Genetic Services, by such Individual or any Family Member of such Individual.

(2) Any reference in this Security Document to Genetic Information concerning an Individual or Family Member of an Individual will 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.

(3) Genetic Information excludes information about the sex or age of any Individual.

Genetic Services – Genetic Services means: (1) A Genetic Test; (2) Genetic Counseling (including obtaining, interpreting, or assessing Genetic Information); or Genetic education.

Genetic Test – Genetic Test means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic Test does not include an analysis of proteins or metabolites that is directly related to a Manifested disease, disorder, or pathological condition.

Group Health Plan – An employee welfare benefit plan (as defined in the Employee Retirement Income and Security Act of 1974), including insured and self insured plans, to the extent that the plan provides medical care, including items and services paid for as medical care, to participants or their dependents directly or through insurance, reimbursement, or otherwise, that:

- Has 50 or more Individuals, or
- Is administered by an entity other than the employer that established and maintains the plan.

Health Care – The provision of care, services, or supplies to a patient includes any:

- preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, counseling, service, or procedure with respect to the physical or mental condition, or functional status, of a patient or affecting the structure or function of the body; and/or
- sale or dispensing of a drug, device, equipment, or other item pursuant to a prescription.

Health Care Clearinghouse – A public or private entity that conducts either of the following:

- Processes or facilitates the processing of Health Information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard Transaction; or
- Receives a standard Transaction from another entity and processes or facilitates the processing of Health Information into nonstandard format or nonstandard data content for the receiving entity.

Health Care Operations – Any of the following activities of the Covered Entity to the extent that the activities are related to Covered Functions:

- Conducting quality assessment and improvement activities, including evaluating outcomes, and developing clinical guidelines;
- Reviewing the competence or qualifications of Health Care professionals, evaluating practitioner and provider performance, Health Plan performance, conducting Training programs in which undergraduate and graduate students and trainees in all areas of Health Care learn under supervision to practice as Health Care Providers (*e.g.*, residency programs, grand rounds, nursing practicums), accreditation, certification, licensing or credentialing activities;
- Insurance rating and other insurance activities relating to the renewal of a contract for insurance, including underwriting, experience rating, and reinsurance, but only when the Individuals are already enrolled in the Health Plan conducting such activities and only when the Use or Disclosure of such Protected Health Information relates to an existing contract of insurance (including the renewal of such a contract);
- Conducting or arranging for medical review, legal services, auditing services, 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 entity, including formulary development and administration, development or improvement of methods of Payment or coverage policies; and
- Business management and general administrative activities of the entity, including, but not limited to:
    - Management activities relating to implementation of and compliance with HIPAA;
    - Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that Protected Health Information is not disclosed to such policy holder, plan sponsor, or customer;
    - Resolution of internal grievances;
    - The sale, transfer, merger, or consolidation of all or part of the Covered Entity with another Covered Entity, or an entity that following such activity will become a Covered Entity and due diligence related to such activity; and
    - Consistent with the applicable requirements of creating de-identified Health Information or a Limited Data Set, and fundraising for the benefit of the

Covered Entity.

Health Care Provider – A provider of medical or health services and any other person or organization that furnishes, bills, or is paid for Health Care in the normal course of business.

Health Information – Any information, including Genetic Information, whether oral or recorded in any form or medium, that is created or received by a Health Care Provider, Health Plan, Public Health Authority, employer, life insurer, school or university, or Health Care Clearinghouse; and that relates to the past, present, or future physical or mental health or condition of an Individual, the provision of Health Care to an Individual, or the past, present, or future Payment for the provision of Health Care to an Individual.

Health Insurance Issuer – An insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State Law that regulates insurance. Such term does not include a Group Health Plan.

Health Maintenance Organization (HMO) – A federally qualified HMO, an organization recognized as an HMO under State Law, or a similar organization regulated for solvency under State Law in the same manner and to the same extent as such an HMO.

Health Plan – An Individual plan or Group Health Plan that provides, or pays the cost of medical care. A Health Plan includes the following, singly or in combination:

- A Group Health Plan;
- A Health Insurance Issuer;
- An HMO;
- Part A or Part B of the Medicare program;
- The Medicaid program;
- The Voluntary Prescription Drug Benefit Program under Part D of Medicare;
- An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy;
- An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers;
- The Health Care program for uniformed services;
- The veterans Health Care program;
- TRICARE, formerly known as The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS);
- The Indian Health Service program under the Indian Health Care Improvement Act;
- The Federal Employees Health Benefits Program;
- An approved State child Health Plan, providing benefits for child health assistance;
- The Medicare Advantage Program under Part C;
- A high risk pool that is a mechanism established under State Law to provide health insurance coverage or comparable coverage to eligible Individuals; and
- Any other Individual or group plan, or combination of Individual or group plans, that provides or pays for the cost of medical care.

A Health Plan excludes:

- Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits; and
- A government-funded program (other than one listed in the above paragraph of this definition) whose principal purpose is other than providing, or paying the cost of, Health Care; or whose principal activity is:
    - The direct provision of Health Care to persons; or
    - The making of grants to fund the direct provision of Health Care to persons.

HHS – The Department of Health and Human Services.

HIPAA – The Health Insurance Portability and Accountability Act of 1996, as amended, and any regulations promulgated thereunder, as may be amended and in effect from time to time.

HIPAA Privacy Officer– The HIPAA Privacy Officer (or Privacy Official) is the person responsible for the development and implementation of the Plan's privacy policies and procedures.

HIPAA Rules – The applicable Privacy or Security regulations promulgated under HIPAA, as may be amended and in effect from time to time.

HIPAA Security Officer – The HIPAA Security Officer (or Security Official) is the person responsible for the development and implementation of the Plan's Security policies and procedures.

Implementation Specification – Specific requirements or instructions for implementing a standard.

Individual – The person who is the subject of Protected Health Information.

Individually Identifiable Health Information – Information that is a subset of Health Information, including demographic information collected from an Individual, and:

- Is created or received by a Health Care Provider, Health Plan, employer, or Health Care Clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an Individual; the provision of Health Care to an Individual; or the past, present, or future Payment for the provision of Health Care to an Individual; and
- That identifies the Individual; or
- With respect to which there is a reasonable basis to believe the information can be used to identify the Individual.

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.

Information Technology (IT) Responsibilities Policy – Policy Number 16:01:00.

Integrity – The property that data or information have not been altered or destroyed in an unauthorized manner.

IT Guidelines – Collectively, the Standard for IT Hardware Asset Management, the IT Hardware Asset Disposal Procedure, the IT Systems Disaster Recovery Standard, the Oxy Cyber Security Incident Response Plan, and the Standard for Smart Devise Use.

IT Hardware Asset Disposal Procedure – Procedure Number IT-ICS-ST-90-0114.

IT Security Policy – The Information Technology (IT) Responsibilities Policy together with the Digital Information Security Policy.

IT Security Policies and IT Guidelines – Collectively, the IT Security Policy and the IT Guidelines.

IT Systems Disaster Recovery Standard – Procedure Number IT-ICS-ST-90-0114.

Law Enforcement Official – An officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

- Investigate or conduct an official inquiry into a potential violation of law; or
- Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Limited Data Set – Protected Health Information that excludes the following direct identifiers of the Individual or of relatives, employers, or household members of the Individual:

- 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.

Malicious Software – Software, for example, a virus, designed to damage or disrupt a system.

Manifestation or Manifested – Manifestation or manifested means, with respect to a disease, disorder, or pathological condition, that an Individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a Health Care professional with appropriate training and expertise in the field of medicine involved. For purposes of this definition, a disease, disorder, or pathological condition is not manifested if the diagnosis is

based principally on Genetic Information.

Minimum Necessary – The minimum amount of Health Information necessary to accomplish the intended purpose of the Use or Disclosure is used or disclosed except in the following situations:

- Disclosures or requests by a health provider for Treatment;
- When an Individual requests the Health Plan, Health Care Provider, or other Covered Entity to use or disclose his/her information under the Authorization procedure;
- When the Individual requests access to his/her own Protected Health Information in Designated Record Sets;
- When the Secretary requests access to the information to ensure compliance or investigate a complaint;
- When Required by Law or permitted (the instances set forth above in the section on permissible Disclosures); and
- When the information is made by a Health Care Provider to the Health Plan pursuant to a request for compliance audit and related purposes.

More Stringent – In the context of a comparison of a provision of State Law and a standard, requirement, or Implementation Specification, a State Law that meets one or more of the following criteria:

- With respect to a Use or Disclosure, the law prohibits or restricts a Use or Disclosure in circumstances under which such Use or Disclosure otherwise would be permitted, except if the Disclosure is:
    - Required by the Secretary in connection with determining whether a Covered Entity or Business Associate is in compliance with this subchapter; or
    - To the Individual who is the subject of the Individually Identifiable Health Information.
- With respect to the rights of an Individual, who is the subject of the Individually Identifiable Health Information regarding access to or amendment of Individually Identifiable Health Information, permits greater rights of access or amendment;
- With respect to information to be provided to an Individual who is the subject of the Individually Identifiable Health Information about a Use, a Disclosure, rights, and remedies, provides the greater amount of information;
- With respect to the form, substance, or the need for express legal permission from an Individual, who is the subject of the Individually Identifiable Health Information, for Use or Disclosure of Individually Identifiable Health Information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission;
- With respect to recordkeeping or requirements relating to accounting of Disclosures, provides for the retention or reporting of more detailed information or for a longer duration; and
- With respect to any other matter, provides greater privacy protection for the Individual who is the subject of the Individually Identifiable Health Information.

Organized Health Care Arrangement – An Organized Health Care Arrangement includes any of the following:

- A clinically integrated care setting in which Individuals typically receive Health Care from more than one Health Care Provider;
- An organized system of Health Care in which more than one Covered Entity participates, and in which the participating covered entities:
    - Hold themselves out to the public as participating in a joint arrangement; and
    - Participate in joint activities that include at least one of the following:
        - Utilization review, in which Health Care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
        - Quality assessment and improvement activities, in which Treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
    - Payment activities, if the financial risk for delivering Health Care is shared, in part or in whole, by participating covered entities through the joint arrangement and if Protected Health Information created or received by a Covered Entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
- A Group Health Plan and a Health Insurance Issuer or HMO with respect to such Group Health Plan, but only with respect to Protected Health Information created or received by such Health Insurance Issuer or HMO that relates to Individuals who are or who have been Individuals or beneficiaries in such Group Health Plan;
- A Group Health Plan and one or more other Group Health Plans each of which are maintained by the same plan sponsor; or
- The Group Health Plans and Health Insurance Issuers or HMOs with respect to such Group Health Plans, but only with respect to Protected Health Information created or received by such Health Insurance Issuers or HMOs that relates to Individuals who are or have been Individuals or beneficiaries in any of such Group Health Plans.

Oxy Cyber Security Incident Response Plan - Procedure Number IT-Sec-ST-99-0129.

Password – Confidential Authentication information composed of a string of characters.

Payment – Activities undertaken by a Health Plan (or by a Business Associate on behalf of a Health Plan) to determine its responsibilities for coverage under the Health Plan policy or contract including the actual Payment under the policy or contract, or by a Health Care Provider (or by a Business Associate on behalf of a provider) to obtain reimbursement for the provision of Health Care. Payment activities include, but are not limited to:

- Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
- Risk adjusting amounts due based on enrollee health status and demographic characteristics;

- Billing, claims management, collection activities, obtaining Payment under a contract for reinsurance (including stop-loss insurance and excess of 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 Protected Health Information relating to collection of premiums or reimbursement:
    - Name and address;
    - Date of birth;
    - Social Security number;
    - Payment history;
    - Account number; and
    - Name and address of the Health Care Provider and/or Health Plan.

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.

Privacy or Privacy Rule – The HIPAA Rules governing the protection of Individually Identifiable Health Information.

Protected Health Information (PHI) – Individually Identifiable Health Information that is transmitted by Electronic Media, maintained in any medium, or transmitted or maintained in any other form or medium, by a Covered Entity. PHI excludes Individually Identifiable Health Information:

- in education records defined and covered by the Family Educational Right and Privacy Act for students in primary and secondary education;
- employment records held by a Covered Entity in its role as employer; and
- regarding a person who has been deceased for more than 50 years.

Public Health Authority – An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Record – Any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for a Covered Entity.

Required by Law – A mandate contained in law that compels an entity to make a Use or Disclosure of Protected Health Information and that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to Health Care Providers participating in the program; and statutes or regulations that require the production of information, including

statutes or regulations that require such information if Payment is sought under a government program providing public benefits.

Routine – Protected Health Information disclosed for the purpose of Treatment, Payment and Health Care Operations.

Sanctions – Sanctions against members of its Workforce who fail to comply with the Employer's Group Health Plan's policies and procedures on Protected Health Information or with the privacy or Security requirements in connection with Protected Health Information held by the Health Plan or its Business Associates.

Secretary – The Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Security or Security Rule – The HIPAA Rules governing the Administrative, Physical and Technical Safeguards applicable to Individually Identifiable Health Information.

Security Measures – The administrative, physical and Technical Safeguards in an Information System.

Security Incident – The attempted or successful unauthorized access, Use, Disclosure, modification, or destruction of information or interference with systems operations in an Information System.

Standard – A rule, condition, or requirement: (1) describing the following information for products, systems, services or practices: (i) classification of components, (ii) specification of materials, performance or operations, or (iii) delineation of procedures; or (2) with respect to the Privacy of Individually Identifiable Health Information.

Standard for IT Hardware Asset Management – Procedure Number IT-ITS-ST-99-0128.

Standard for Smart Device Use – Procedure Number IT-ITS-ST-99-0216.

State – The 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

State Law – A constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

Subcontractor – a person who acts on behalf of a Business Associate, other than in the capacity of a member of the Workforce of such Business Associate.

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

Training – Training persons in the Workforce who are likely to obtain access to Protected Health Information or electronic Protected Health Information on the Health Plan's policies and procedures, required under the HIPAA privacy and Security regulations that is relevant to their activities.

Transaction – The transmission of information between two parties to carry out financial or administrative activities related to Health Care. A Transaction would mean any of the following:

- Health claims or equivalent encounter information. This Transaction could be used to submit Health Care claim billing information, encounter information, or both, from Health Care Providers to payers, either directly or via intermediary billers and claims clearinghouses;
- Health Care Payment and remittance advice. This Transaction could be used by a Health Plan to make a Payment to a financial institution for a Health Care Provider (sending Payment only), to send an explanation of benefits remittance advice directly to a Health Care Provider (sending data only), or to make Payment and send an explanation of benefits remittance advice to a Health Care Provider via a financial institution (sending both Payment and data);
- Coordination of benefits. This Transaction could be used to transmit Health Care claims and billing Payment information between payers with different Payment responsibilities where coordination of benefits is required or between payers and regulatory agencies to monitor the furnishing, billing, and/or Payment of Health Care services within a specific Health Care/insurance industry segment;
- Health claims status. This Transaction could be used by Health Care Providers and recipients of Health Care products or services (or their authorized agents) to request the status of a Health Care claim or encounter from a Health Plan;
- Enrollment and disenrollment in a Health Plan. This Transaction could be used to establish communication between the sponsor of a health benefit and the payer. It provides enrollment data, such as subscriber and dependents, employer information, and primary care Health Care Provider information. A sponsor would be the backer of the coverage, benefit, or product. A sponsor could be an employer, union, government agency, association, or insurance company. The Health Plan would refer to an entity that pays claims, administers the insurance product or benefit, or both;
- Eligibility for a Health Plan. This Transaction could be used to inquire about the eligibility, coverage, or benefits associated with a benefit plan, employer, plan sponsor, subscriber, or a dependent under the subscriber's policy. It also could be used to communicate information about or changes to eligibility, coverage, or benefits from information sources (such as insurers, sponsors, and payers) to information receivers (such as physicians, hospitals, third party administrators, and government agencies);
- Health Plan premium Payments. This Transaction could be used by, for example, employers, employees, unions, and associations to make and keep track of Payments of Health Plan premiums to their health insurers. This Transaction could also be used by a Health Care Provider, acting as liaison for the beneficiary, to make Payment to a health insurer for coinsurance, co-Payments, and deductibles;
- Referral certification and Authorization. This Transaction could be used to transmit Health Care service referral information between Health Care Providers, Health Care Providers furnishing services, and payers. It could also be used to obtain Authorization for certain Health Care services from a Health Plan;
- First report of injury. This Transaction could be used to report information pertaining to an injury, illness, or incident to entities interested in the information for statistical, legal, claims, and risk management processing requirements;
- Health claims attachments. This Transaction could be used to transmit Health Care service information, such as subscriber, patient, demographic, diagnosis, or

Treatment data for the purpose of a request for review, certification, notification, or reporting the outcome of a Health Care services review; and

- Other Transactions as the Secretary may prescribe by regulation. The Secretary may adopt Standards, and data elements for those Standards, for other financial and administrative Transactions deemed appropriate by the Secretary. These Transactions would be consistent with the goals of improving the operation of the Health Care system and reducing administrative costs.

Treatment – The provision, coordination, or management of Health Care and related services by one or more Health Care Providers, including 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 - PHI that is not rendered unusable, unreadable, or indecipherable to authorized Individuals through the use of technology or methodology specified by the Secretary in the guidance issued under Section 13402(h)(2) of Pub.L.111-5 on the HHS website. Unsecured PHI includes information in any form or medium, including electronic, paper or oral form.

PHI is rendered unusable, unreadable, or indecipherable to authorized Individuals if one or more of the following applies:

(1) Electronic PHI has been encrypted as specified in the Security Rule by the use 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 and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

   a. Valid encryption processes for data at rest (i.e., data that resides in databases, file systems, flash drives, memory, and any other structured storage systems) are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.

   b. Valid encryption processes for data in motion (i.e., data that is moving through a network, including wireless transmission, whether by e-mail or structured electronic interchange) are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards FIPS) 140-2 validated.

(2) The media on which the PHI is stored or recorded have been destroyed in one of the following ways:

   a. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

b. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

Use – The sharing, employment, application, utilization, examination or analysis of Individually Identifiable Health Information within an entity that holds the information.

User – A person or entity with authorized access.

Workforce – The employees, volunteers, trainees and other persons under the direct control of a Covered Entity, including persons providing labor on an unpaid basis.

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.

Covered Entity List

Occidental Petroleum Corporation Welfare Plan (Medical, Dental and FSA components)

Occidental Petroleum Corporation Retiree Medical Plan

Occidental Petroleum Corporation Retiree Dental Plan

Occidental Petroleum Corporation Health Promotion Plan

Occidental Chemical Corporation Medical Plan

Occidental Chemical Corporation Retiree Medical Plan

Occidental Chemical Corporation Retiree Dental Plan

Occidental Chemical Corporation Dental Assistance Plan

Occidental Chemical Corporation Pretax Premium Plan

Occidental Chemical Corporation Special Welfare Plan for North Tonawanda Hourly Employees

Occidental Chemical Corporation Special Welfare Plan for North Tonawanda Salaried Employees

Blue Cross-Blue Shield Plan for Hourly Employees of Occidental Chemical Corporation at Niagara Falls

Blue Cross-Blue Shield Plan for Hourly Employees of Occidental Chemical and Plastics Corporation - North Tonawanda

Group Insurance Plan for Petrolia Hourly Employees

Group Insurance Plan for Petrolia Hourly Retirees

Appendix C

Business Associate Inventory

See list maintained by Lou Massey.

FORM OF

Business Associate Agreement

By and Between

Occidental Petroleum Corporation

on behalf of the
(Plan name)

and

(Business Associate)

Business Associate Agreement

This Business Associate Agreement ("Agreement") is effective [*Insert Date*] and made by and between Occidental Petroleum Corporation ("Oxy"), a [*Insert State of Incorporation*] corporation, on behalf of the [*Insert Plan Name*] (the "Covered Entity"), and [*Insert Business Associate name*] ("Business Associate"), a [*Insert State of Incorporation*] corporation (collectively, the "Parties"). Terms appearing below in the "Witnesseth" section with initial upper case letters shall have the respective meanings assigned to them in this introductory paragraph or in Section 1.02 of this Agreement, as applicable.

WITNESSETH:

WHEREAS, Business Associate has previously entered into an arrangement with Oxy and/or the Covered Entity to provide Services to or on behalf of the Covered Entity;

WHEREAS, the Parties acknowledge and agree that in providing Services to or on behalf of the Covered Entity, Business Associate will create, receive, use or disclose Protected Health Information;

WHEREAS, the Parties intend to enter into this Agreement to address the requirements of HIPAA, HITECH, the Privacy Rule, and the Security Rule as they apply to "business associates", including the establishment of permitted and required uses and disclosures (and appropriate limitations and conditions on such uses and disclosures) of Protected Health Information by Business Associate that is created or received in the course of performing Services on behalf of the Covered Entity; and

WHEREAS, the objective of this Agreement is to provide Oxy and the Covered Entity with reasonable assurances that Business Associate will appropriately safeguard the Protected Health Information that it creates or receives in the course of providing Services to the Covered Entity;

NOW, THEREFORE, in connection with Business Associate's creation, receipt, use or disclosure of Protected Health Information and in consideration for the mutual promises contained herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties hereby agree as follows:

ARTICLE I
Definitions

1.01 **General Definitions.** All terms appearing in this Agreement with initial upper case letters that are not otherwise defined in this Agreement shall have the same meaning as that provided for the respective terms in 45 C.F.R. §§ 160.103, 164.103, 164.304 and 164.501.

1.02 **Specific Definitions.** For purposes of this Agreement, the following terms shall have the indicated meanings whenever the term appears with initial upper case letters in this Agreement:

(a) **"Business Associate"** shall mean [Name of Business Associate].

(b) **"Breach"** shall mean the acquisition, access, use or disclosure of Protected Health Information in a manner not permitted by HIPAA which compromises the security or privacy of the Protected Health Information unless such acquisition, access, use or disclosure is otherwise excluded under 45 C.F.R. § 164.402. For this purpose, Protected Health Information is "compromised" to the extent that the action poses a significant risk of financial, reputational or other harm to the Individual.

(c) **"Covered Entity"** shall mean the *[Insert Plan name]*

(d) **"Data Aggregation"** shall mean, with respect to Protected Health Information created or received by the Business Associate in its capacity as the Business Associate of the Covered Entity, the combining of such Protected Health Information by the Business Associate with the Protected Health Information received by the Business Associate in its capacity as business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective entities.

(e) **"Designated Record Set"** shall mean a group of records maintained by or for Oxy and/or the Covered Entity within the meaning of 45 C.F.R. § 164.501 that consists of: (i) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (ii) records that are used, in whole or in part, by or for Oxy and/or the Covered Entity to make decisions about Individuals.

For purposes of this Section 1.02(e), the term "record" means any item, collection or grouping of information that includes Protected Health Information and is maintained, collected, used or disseminated by or for the Covered Entity.

(f) **"HHS-Approved Technology"** shall mean, with respect to data in motion, the encryption guidelines in Federal Information Processing Standard 140-2. For data at rest, HHS-Approved Technology shall mean the encryption guidelines in National Institutes of Standards and Technology (NIST) Special Publication 800-111. With respect to the destruction of data containing Protected Health Information, an HHS-Approved Technology requires the destruction of the media on which the Protected Health Information is stored such that, for paper, film or other hard copy media, destruction requires shredding or otherwise destroying the media so that Protected Health Information cannot be read or reconstructed; for electronic media, destruction requires that the data be cleared, purged or destroyed consistent with NIST Special Publication 800-88 such that the information cannot be retrieved. HHS-Approved Technology may be updated from time to time based on guidance from the Secretary.

(g) **"HIPAA"** shall mean the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191.

(h) **"HITECH"** shall mean the Health Information Technology for Economic and Clinical Health Act, Pub. L. 111-5.

(i) **"Individual"** shall have the same meaning as the term "individual" in 45 C.F.R. § 160.103, and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

(j) **"Privacy Rule"** shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and E.

(k) **"Protected Health Information"** shall mean individually identifiable health information that is transmitted by electronic media (within the meaning of 45 C.F.R. § 160.103), maintained in electronic media, or maintained or transmitted in any form or medium including, without limitation, all information (including demographic, medical, and financial information), data, documentation, and materials that are created or received by Business Associate from or on behalf of the Covered Entity in connection with the performance of Services, and 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 that identifies or could reasonably be used to identify an Individual and shall otherwise have the meaning given to such term under the Privacy Rule including, but not limited to, 45 C.F.R. § 160.103. Protected Health Information does not include health information that has been de-identified in accordance with the standards for de-identification provided for in the Privacy Rule including, but not limited to, 45 C.F.R. § 164.514.

(l) **"Required By Law"** shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103.

(m) **"Secretary"** shall mean the Secretary of the United States Department of Health and Human Services ("HHS") or his designee.

(n) **"Secured Protected Health Information"** shall mean Protected Health Information to the extent that the information is protected by using an HHS-Approved Technology identified by HHS for rendering Protected Health Information unusable, unreadable or indecipherable to unauthorized individuals.

(o) **"Security Rule"** shall mean the Security Standards at 45 C.F.R. Part 160, Part 162, and Part 164.

(p) **"Services"** shall mean the functions, activities or services to be provided to Oxy and/or the Covered Entity under the terms of an arrangement between Oxy and/or the Covered Entity and Business Associate.

(q) **"Unsecured Protected Health Information"** shall mean Protected Health Information that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of an HHS-Approved Technology.

ARTICLE II
Obligations and Activities of Business Associate

2.01 **Non-Disclosure of Protected Health Information.** Business Associate agrees not to use or disclose Protected Health Information other than as permitted or required by this Agreement or as Required By Law.

2.02 **Safeguards.** Business Associate agrees to use appropriate safeguards to prevent use or disclosure of Protected Health Information other than as provided for by this Agreement or the Privacy Rule. Business Associate agrees to implement administrative, physical, and technical safeguards, along with policies and procedures, that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic Protected Health Information that it creates, receives, maintains or transmits on behalf of the Covered Entity and to utilize Secured Protected Health Information in connection with the performance of Services under this Agreement.

2.03 **Mitigation.** Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate relating to a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement or that would otherwise cause a Breach of Unsecured Protected Health Information.

2.04 **Reporting of Violations.** Subject to Section 2.05, Business Associate agrees to report to Oxy and the Covered Entity any use or disclosure of Protected Health Information not provided for by this Agreement within thirty (30) days of such disclosure or Business Associate's knowledge of such disclosure. Business Associate agrees to report to Oxy and the Covered Entity any security incident (within the meaning of 45 C.F.R. § 164.304) of which Business Associate becomes aware.

2.05 **Breach of Unsecured Protected Health Information.** To the extent that the Business Associate knows or has reason to know that there has been a Breach or suspected Breach of Unsecured Protected Health Information, the Business Associate is required to identify the Individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, acquired, accessed, used or disclosed and to notify Oxy and the Covered Entity of such Breach without reasonable delay, but no later than five (5) days after discovery of the Breach. Upon discovering the Breach, the Business Associate is required to (a) identify the entity to which the information was impermissibly disclosed, (b) determine whether or not the entity is subject to HIPAA and the Privacy Rule, (c) identify the type and amount of Protected Health Information disclosed, (d) determine whether the disclosure poses a significant risk of financial, reputational, or other harm to the Individual, and (e) if the improperly disclosed Unsecured Protected Health Information is returned, determine if the information was returned before being accessed for an improper purpose.

2.06 **Notice of a Breach of Unsecured Protected Health Information**. In the event of a Breach involving Unsecured Protected Health Information, the Business Associate, with the prior written approval of Oxy and the Covered Entity, will notify the affected Individuals without unreasonable delay, but no later than sixty (60) days after discovery of the Breach ("notice date"). The notice will include (a) a brief description of the incident, (b) the date the Breach occurred, (c) the date the Breach was discovered, (d) the type of Protected Health Information involved, (e) steps the Individual should take to protect him/herself from potential harm resulting from the Breach, (f) a brief description of steps the Covered Entity has taken to investigate, mitigate losses and protect against further Breaches, and (g) contact information for Individuals to ask questions, including a toll-free number, e-mail address, website or postal address. To the extent that the Breach involves more than 500 residents of a single state or jurisdiction, the Business Associate shall provide to Covered Entity, [no later than the notice date], the information necessary for the Covered Entity to prepare the notice to media outlets as set forth in 45 C.F.R. § 164.406. To the extent that the Breach involves 500 or more Individuals, the Business Associate shall provide to the Covered Entity, [no later than the notice date], the information necessary for the Covered Entity to prepare the notice to the Secretary of HHS, as set forth in 45 C.F.R. § 164.408. To the extent that the Breach involves less than 500 Individuals, the Business Associate shall maintain a log of such Breaches and provide such log to the Covered Entity for submission to HHS. The Breach log shall be provided by Business Associate to the Covered Entity on an annual basis, not later than sixty (60) days after the end of the calendar year.

2.07 **Audits**. Business Associate shall permit Oxy and the Covered Entity to audit Business Associate's compliance with the Privacy Rule, Security Rule and this Agreement upon reasonable prior notice and in a reasonable manner. Oxy and/or the Covered Entity shall pay for any such audits.

2.08 **Agents and Contractors**. Business Associate agrees to ensure that any Business Associate agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Oxy and/or the Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information. Business Associate also agrees to ensure that any Business Associate employee or agent, including any subcontractor to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Oxy and/or the Covered Entity agrees to implement reasonable and appropriate safeguards to protect such Protected Health Information. Business Associate, Oxy, and the Covered Entity agree that the Business Associate is not the agent of the Covered Entity or Oxy at any time under this Agreement.

2.09 **Sanctions**. Business Associate agrees to apply appropriate sanctions against any Business Associate employee or agent, including a subcontractor, with access to Individuals' Protected Health Information who fails to comply with Oxy's, the Covered Entity's, or the Business Associate's health information privacy policies and procedures.

2.10 **Amendment of Protected Health Information**. Business Associate agrees to make appropriate amendments to Protected Health Information in a Designated Record Set that either the Covered Entity or an Individual requests pursuant to procedures established under 45 C.F.R. § 164.526. To the extent Business Associate is

requested by an Individual to amend his or her Protected Health Information, Business Associate shall communicate its approval or denial of such request to the Individual pursuant to procedures to be mutually agreed upon in advance by the Parties.

2.11 **Disclosure of Internal Practices, Books, and Records.** Business Associate agrees to make internal practices, books, and records (including policies and procedures) relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of Oxy or the Covered Entity, available to the Covered Entity or, at the request of the Covered Entity, to the Secretary, in a time and manner mutually agreed to by the Parties or designated by the Secretary, for purposes of determining the Covered Entity's compliance with the Privacy Rule.

2.12 **Access to Protected Health Information.** To the extent that either the Covered Entity or an Individual requests to inspect or obtain a copy of Protected Health Information (as provided for in 45 C.F.R. § 164.524) that may be in the possession or control of the Business Associate or its agents or subcontractors, or that exists in a Designated Record Set, Business Associate shall respond within thirty (30) days of its receipt of the request by Business Associate, provided that compliance with the request would not result in a violation of HIPAA or the Privacy Rule.

2.13 **Documentation of Disclosures.** Business Associate agrees to document disclosures of Protected Health Information and information related to such disclosures as would be required for a Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528. At a minimum, such documentation shall include: (i) the date of each disclosure; (ii) the name of the entity or person who received Protected Health Information and, if known, the address of the entity or person; (iii) a brief description of the Protected Health Information disclosed; (iv) the disclosures of Protected Health Information that occurred during the six-year period prior to the date of the request for an accounting (or any shorter period of time requested by the Individual) and that are otherwise subject to the accounting requirement in 45 C.F.R. § 164.528; and (v) a brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure or, if applicable, in lieu of such a statement, a copy of the Individual's authorization and a copy of the written request for disclosure.

2.14 **Accounting for Disclosures.** Business Associate agrees to provide to the Covered Entity or an Individual, in a time and manner mutually determined by the Parties, information collected in accordance with Section 2.13 of this Agreement so as to permit the Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528, provided, however, that to the extent that the Covered Entity uses or maintains an electronic health record with respect to Protected Health Information, Business Associate shall provide such accounting to the Individual (or, upon the request of the Covered Entity, to the Covered Entity for delivery to the Individual) of the disclosures required for the three-year period immediately preceding the date on which the accounting is requested. The accounting of disclosures through electronic health records shall not be required earlier than the earliest applicable date established by the Secretary of HHS.

2.15 **Facilitate the Exercise of Privacy Rights.** Business Associate agrees to establish procedures that allow Individuals to exercise their rights under the Privacy Rule, including the right to (i) inspect and obtain copies of records and documents within the possession or control of the Business Associate that contain the Individual's Protected Health Information; (ii) request amendments to their Protected Health Information; (iii) receive an accounting of disclosures of their Protected Health Information by Business Associate; (iv) request restrictions on the use or disclosure of Protected Health Information; and (v) receive communications regarding Protected Health Information at alternative locations or by alternative means. Business Associate agrees that, to the extent that an Individual requests restrictions with respect to the disclosure of Protected Health Information, and such restrictions relate to disclosure to the Covered Entity for purposes of carrying out payment or health care operations (but not treatment), and the Protected Health Information pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full, such restriction shall be followed.

2.16 **No Waiver of Rights.** Business Associate agrees to not require Individuals to waive their health information privacy rights as a condition for treatment, payment or enrollment in the Covered Entity, or eligibility for its benefits.

2.17 **Responses to Subpoenas.** In the event that Business Associate receives a subpoena, discovery request or other lawful process, with or without an order from a court or administrative tribunal, arising out of or in connection with the Covered Entity or this Agreement including, but not limited to, any use or disclosure of Protected Health Information or any failure in Business Associate's health data security measures, Business Associate shall fully comply with the notice and protective action obligations set forth in 45 C.F.R. § 164.512(e) in accordance with Business Associate's standard policy and procedures regarding subpoenas, discovery requests, and other lawful processes which shall be communicated to the Covered Entity upon request.

2.18 **Electronic Transactions.** To the extent required under HIPAA (including the Standards for Electronic Transactions at 45 C.F.R. Parts 160 and 162), Business Associate agrees to use or conduct, in whole or part, standard transactions and utilize code sets or identifiers under the Privacy Rule for or on behalf of Oxy or the Covered Entity as detailed under the Privacy Rule or HIPAA (including the Standards for Electronic Transactions at 45 C.F.R. Parts 160 and 162). Business Associate shall also require any subcontractor or agent to also comply with such electronic transaction requirements under HIPAA (including the Standards for Electronic Transactions at 45 C.F.R. Parts 160 and 162).

2.19 **Security Standards.** Business Associate acknowledges that it may need to issue and change procedures from time to time to improve electronic data and file security, and agrees that such measures shall be at least as stringent as may be required by the Privacy Rule or the Security Rule, as applicable. Notwithstanding the foregoing, Business Associate agrees and acknowledges that it shall at all times use an HHS-Approved Technology for all Protected Health Information that is in motion, stored or to be destroyed.

2.20 **Disclosures to Designated Plan Sponsor Representatives.** Oxy shall identify for Business Associate, in writing, certain Oxy employees who are authorized to discuss Protected Health Information with Business Associate in connection with an

Individual's claim for benefits from the Covered Entity. To the extent that Business Associate is contacted by any such designated Oxy representative in connection with an Individual's claim for benefits from the Covered Entity, Business Associate shall treat such inquiry as relating to "treatment, payment or healthcare operations" within the meaning of the Privacy Rule and shall provide the information permitted under such Privacy Rule.

2.21 **Notice of Privacy Practices.** Covered Entity shall prepare and distribute a notice of privacy practices as required by the Privacy Rule. If Business Associate maintains a web site on behalf of Oxy or the Covered Entity that provides information about the Covered Entity's participant services or benefits, Business Associate shall make the notice of privacy practices available electronically through the web site and shall make certain that the notice of privacy practices is prominently posted on the web site.

ARTICLE III
Permitted Uses and Disclosures By Business Associate

3.01 **General Uses and Disclosures.** Except as otherwise limited by this Agreement, Business Associate agrees to create, receive, use or disclose Protected Health Information only in a manner that is consistent with this Agreement, the Privacy Rule and the Security Rule, and only in connection with providing Services to Oxy and/or the Covered Entity, provided that such creation, receipt, use or disclosure would not violate the Privacy Rule or Security Rule if done by the Covered Entity, or the minimum necessary policies and procedures of the Covered Entity.

3.02 **Use and Disclosure for Treatment, Payment and Health Care Operations.** In providing Services, Business Associate shall be permitted to use and disclose Protected Health Information for purposes of "treatment, payment and health care operations" in accordance with the Privacy Rule, including, but not limited to, using or disclosing Protected Health Information (i) to investigate, pay, audit and otherwise administer and facilitate the payment of health plan claims; (ii) to enroll or disenroll participants and beneficiaries in and/or confirm or deny participant and beneficiary eligibility for participation in the Covered Entity; and (iii) to coordinate the payment of benefits from the Covered Entity when a participant or beneficiary is enrolled in another health plan which provides similar benefits, provided, however, that any communication by Business Associate that is about a product or service and that encourages recipients of the communication to purchase or use the product or service shall not be considered a health care operation for purposes of 45 C.F.R. Part 164, subpart E, unless the communication is made in accordance with 45 C.F.R. § 164.501 and is approved in writing by Covered Entity.

3.03 **Use and Disclosure for Public Health, Health Oversight and Law Enforcement Purposes.** In providing Services, Business Associate shall be permitted to use and disclose Protected Health Information, in accordance with the Privacy Rule, (i) to provide needed information to government agencies engaged in public health, health oversight, law enforcement, and otherwise as Required by Law; and (ii) to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.502(j)(1).

3.04 **Use for Management and Administration of Business Associate.** Except as otherwise limited in this Agreement, Business Associate may use Protected Health

Information for the proper management and administration of the Business Associate (defined as those uses arising in the ordinary course of its business and as is customary in its industry) or to carry out the legal responsibilities of the Business Associate. Any such use shall be in accordance with the uses and disclosures permitted by the Privacy Rule.

3.05 **Disclosure for Management and Administration of Business Associate.** Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate provided that the disclosures are Required by Law, or Business Associate (i) obtains the prior written approval of the Covered Entity for such use or disclosure, and (ii) obtains reasonable assurances from the person to whom the information is to be disclosed that (A) the information shall remain confidential, (B) the information shall be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and (C) the person shall notify the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

3.06 **Use for Data Aggregation Services.** Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services relating to the health care operations of the Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

3.07 **Prohibition on Sale of Electronic Health Records or Protected Health Information.** Except as provided in this Agreement or otherwise excepted under HITECH, Business Associate shall not directly or indirectly receive remuneration in exchange for any Protected Health Information of an Individual unless the Covered Entity or Business Associate has received a valid authorization (within the meaning of 45 C.F.R. § 164.508) that includes a specification that the Protected Health Information can be further exchanged for remuneration by the entity receiving the Protected Health Information of that Individual.

ARTICLE IV
Obligations of the Covered Entity

4.01 **Obligations to Notify Business Associate.**

(a) **Limitations in Notice of Privacy Practices.** Covered Entity shall notify Business Associate of any limitations in the Covered Entity's notice of privacy practices provided in accordance with the requirements of 45 C.F.R. § 164.520, to the extent such limitations may affect Business Associate's use or disclosure of Protected Health Information.

(b) **Changes in Permission by Individual for Use of Disclosure.** Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, if and to the extent that such changes affect Business Associate's use or disclosure of Protected Health Information.

(c) **Agreements to Restrict Use or Disclosure.** Covered Entity shall notify Business Associate of any restrictions on the use or disclosure of Protected Health Information or a request for confidential communication that the

Covered Entity has agreed to pursuant to and in accordance with the requirements of 45 C.F.R. § 164.522, or shall direct Individuals to make any such request directly to Business Associate if and to the extent that such restriction or request may affect Business Associate's use or disclosure of Protected Health Information.

4.02 **Permissible Requests by Covered Entity.** Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule or Security Rule if done by the Covered Entity, except that the Covered Entity may request that Business Associate perform Data Aggregation services pursuant to the provisions of Section 3.06 of this Agreement.

ARTICLE V
Term and Termination

5.01 **Term.** This Agreement shall terminate when all of the Protected Health Information provided by the Covered Entity to Business Associate, or created or received by Business Associate on behalf of the Covered Entity, is destroyed or returned to the Covered Entity or, if it is infeasible to return or destroy Protected Health Information, protections shall be extended to such information, in accordance with the termination provisions in this Article V.

5.02 **Termination for Cause.** Upon the Covered Entity's knowledge of a material breach of this Agreement by Business Associate, the Covered Entity shall either (i) provide an opportunity for Business Associate to cure the breach or end the violation, and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time agreed to by the Parties; or (ii) immediately terminate this Agreement if a cure is not possible.

5.03 **Effect of Termination.**

(a) **Return or Destruction of Protected Health Information.** Except as provided in Section 5.03(b) of this Agreement, upon termination of this Agreement for any reason, Business Associate shall return or destroy (in accordance with the HHS-Approved Technology) all Protected Health Information received from the Covered Entity, or created or received by Business Associate on behalf of the Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(b) **Extension of Protections for Retained Protected Health Information.** In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to the Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business

Associate maintains such Protected Health Information. The obligations of the Business Associate under this Agreement shall survive termination of this Agreement with respect to that Protected Health Information that Business Associate is unable to return or destroy.

ARTICLE VI
Miscellaneous

6.01 **Regulatory References.** A reference in this Agreement to a section in the Privacy Rule or the Security Rule means the section in the respective regulations, as amended and in effect at the relevant time.

6.02 **Amendment.** The Parties agree to take such action as is necessary to amend this Agreement from time to time in order for the Covered Entity to comply with the requirements of the Privacy Rule, the Security Rule, and HIPAA. All references to "C.F.R." are to the Code of Federal Regulations as amended and in effect at the relevant time.

6.03 **Survival.** The respective rights and obligations of Business Associate under Articles V and VI of this Agreement shall survive the termination of this Agreement.

6.04 **Interpretation.**

(a) **Ambiguity.** Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the Covered Entity to comply with the Privacy Rule or the Security Rule, as applicable.

(b) **Inconsistency.** In the event of an inconsistency between the provisions of this Agreement and the Privacy Rule or the Security Rule, as may be amended from time to time, as a result of interpretations by HHS, a court or another regulatory agency with authority over the Parties, the interpretation of HHS, such other court or regulatory agency shall prevail.

(c) **Non-Mandatory Provisions.** In the event provisions of this Agreement are not the same as those mandated by the Privacy Rule or the Security Rule, but are nonetheless permitted by the Privacy Rule or the Security Rule, the provisions of this Agreement shall control.

6.05 **Complete Integration.** This Agreement constitutes the entire agreement between the Parties with respect to HIPAA, the Privacy Rule, and the Security Rule, and supersedes all prior negotiations, discussions, representations or proposals, whether oral or written, unless expressly incorporated herein, related to the subject matter of the Agreement. Unless expressly provided otherwise herein, this Agreement may not be modified unless in writing signed by the duly authorized representatives of the Parties.

6.06 **Severability.** If any provision or part of this Agreement is found to be invalid, the remaining provisions of this Agreement shall remain in full force and effect.

6.07 **No Third-Party Beneficiaries.** Except as expressly provided for in the Privacy Rule, the Security Rule, and the Agreement, there are no third-party beneficiaries to this

Agreement. Business Associate's obligations, unless expressly noted herein, are only to Oxy and the Covered Entity.

6.08 **Successors and Assigns**. This Agreement shall inure to the benefit of and be binding upon the successors and assigns of Oxy, the Covered Entity, and Business Associate. However, this Agreement is not assignable by any Party without the prior written consent of the other Parties, which shall not be unreasonably withheld, except that (i) Business Associate, the Covered Entity, and Oxy may assign or transfer this Agreement to any entity owned or under common control with Business Associate, the Covered Entity or Oxy, respectively; and (ii) this Agreement shall automatically be assigned to any entity to which the agreement for provision of Services is properly assigned.

6.09 **Confidentiality**. Except as otherwise provided for in the Privacy Rule, the Security Rule, or this Agreement, no Party shall disclose the terms of this Agreement to any third party without the remaining Parties' written consent.

6.10 **Counterparts**. This Agreement may be executed in two or more counterparts, each of which may be deemed an original.

6.11 **Applicable Laws**. Business Associate represents and warrants that it shall comply with all applicable laws and regulatory requirements in the performance of this Agreement. The Parties agree to enter into good faith discussions aimed at amending this Agreement from time to time to comply with the requirements of HIPAA, the Privacy Rule, the Standards for Electronic Transactions at 45 C.F.R. Parts 160 and 162, the Security Rule, and related regulations and technical pronouncements, provided, however, that Business Associate shall also be responsible for complying with any state privacy or data security rules that are not contrary (within the meaning of 45 C.F.R. § 160.202) to HIPAA, the Privacy Rule, the Security Rule and related regulations and technical pronouncements and, to the extent applicable, that are more stringent (within the meaning of 45 C.F.R. §§ 160.202 and 160.203(b)) than a standard, requirement or implementation specification adopted under 45 C.F.R. Part 164.

6.12 **Governing Law**. This Agreement shall be governed by and construed in accordance with the same internal laws governing the Services provided to Oxy or the Covered Entity by Business Associate.

6.13 **Applicability to Separate Covered Entities**. If, and to the extent that this Agreement applies to two or more separate "covered entities" (as defined in the Privacy Rule), the provisions of this Agreement regarding the permitted and required uses and disclosures (and limitations and conditions on such uses and disclosures) of Protected Health Information shall apply separately and independently to each such "covered entity", except to the extent otherwise agreed to by the Parties.

6.14 **Indemnification**. [The Parties agree and acknowledge that except as set forth herein, the indemnification obligations contained under the [Insert Name of Underlying Agreement] will govern each party's performance under this Agreement.]

Oxy, Covered Entity and Business Associate agree to indemnify and hold each other harmless from any and all liability, damages, costs (including reasonable attorneys' fees and costs), fines, penalties and expenses imposed upon or asserted against the

non-indemnifying party arising out of the indemnifying party's or its agents' or subcontractors' use or disclosure of Protected Health Information contrary to the provisions of HIPAA, the Privacy Rule, the Security Rule, HITECH, this Agreement or other applicable law.

[Notwithstanding the foregoing, nothing in this Section 6.14 will limit any rights the Parties may have to additional remedies under the [Insert Name of Underlying Agreement] or under applicable law for any acts or omissions of the Parties.]

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their duly authorized representatives.

THE PARTIES ACKNOWLEDGE THAT THEY HAVE READ THIS AGREEMENT, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS.

Business Associate Name

By: _____

Print Name: _____

Title: _____

Date: _____

Occidental Petroleum Corporation on behalf of the [Insert Plan Name]

By: _____

Print Name: _____

Title: _____

Date: _____

OCCIDENTAL PETROLEUM CORPORATION
AND ITS AFFILIATES AND SUBSIDIARIES

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.

Health Information Privacy

This Notice is required by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and is intended to describe how the Occidental Petroleum Corporation ("Oxy") health plan, (collectively, "Health Plan"), to the extent applicable to you, will protect your health information.

"Health information" for this purpose means information that identifies you and either relates to your physical or mental health condition, or relates to the payment of your health care expenses. This individually identifiable health information is known as "protected health information" ("PHI"). Your PHI will not be used or disclosed without a written authorization from you, except as described in this Notice or as otherwise permitted by federal or state health information privacy laws.

Health Plan Privacy Obligations

The Health Plan is required by law to:

- Make sure that health information that identifies you is kept private;
- Give you this Notice of its legal duties and privacy practices with respect to health information about you;
- Notify you following a breach of your unsecured PHI; and
- Follow the terms of the Notice that are in effect.

How the Health Plan May Use and Disclose Health Information About You

The Health Plan may use health information or disclose it to others for a number of different reasons. The following are the different ways that the Health Plan may use and disclose your PHI without your authorization:

- **For Treatment.** The Health Plan may disclose your PHI to a health care provider who provides, coordinates or manages health care treatment on your behalf. For example, if you are unable to provide your medical history as a result of an accident, the Health Plan may advise an emergency room physician about the different medications that you may have been prescribed.

- **For Payment.** The Health Plan may use and disclose your PHI so claims for health care treatment, services, and supplies that you receive from health care providers may be paid according to the Health Plan's terms. The Health Plan may also use your PHI for billing, reviews of health care services received, and subrogation. For example, the Health Plan may tell a doctor or hospital whether you are eligible for coverage or what percentage of the bill will be paid by the Health Plan.

- **For Health Care Operations.** The Health Plan may use and disclose your PHI to enable it to operate more efficiently or to make certain that all of its participants receive the appropriate health benefits. For example, the Health Plan may use your PHI for case management, to refer individuals to disease management programs, for underwriting (excluding any PHI that is genetic information), premium rating, activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, to arrange for medical reviews, or to perform population-based studies designed to reduce health care costs. In addition, the Health Plan may use or disclose your PHI to conduct compliance reviews, audits, legal reviews, actuarial studies, and/or for fraud and abuse detection. The Health Plan may also combine health information about participants and disclose it to Oxy in a non-identifiable, summary fashion so that Oxy can decide, for example, what types of coverage the Health Plan should provide. The Health Plan may also remove information that identifies you from health information that is disclosed to Oxy so that the health information that is used by Oxy does not identify the specific Health Plan participants.

- **To The Plan Sponsor.** The Health Plan is sponsored by Oxy. The Health Plan may disclose your PHI to designated personnel at Oxy so that they can carry out related administrative functions, including the uses and disclosures described in this Notice. Such disclosures will be made only to the individuals authorized to receive such information under the Health Plan. These individuals will protect the privacy of your health information and ensure that it is used only as described in this Notice or as permitted by law. Unless authorized by you in writing, your health information: (1) may not be disclosed by the Health Plan to any other employee or department of Oxy, and (2) will not be used by Oxy for any employment-related actions or decisions, or in connection with any other employee benefit plans sponsored by Oxy.

- **To a Business Associate.** Certain services are provided to the Health Plan by third-party administrators known as "business associates." For example, the Health Plan may place information about your health care treatment into an electronic claims processing system maintained by a business associate so that your claim may be paid. In so doing, the Health Plan will disclose your PHI to its business associates so that the business associates can perform their claims payment functions. However, the Health Plan will require its business associates, through written agreements, to appropriately safeguard your health information.

- **To Individuals Involved in Your Care or Payment of Your Care.** The Health Plan may disclose PHI to a close friend or family member involved in or who helps pay for your health care. The Health Plan may also advise a family member or close friend about your condition, your location (for example, that you are in the hospital), or death, unless other laws would prohibit such disclosures.

- **As Required by Law.** The Health Plan will disclose your PHI when required to do so by federal, state, or local law, including those laws that require the reporting of certain types of wounds, illnesses or physical injuries.

Special Use and Disclosure Situations

The Health Plan may also use or disclose your PHI without your authorization under the following circumstances:

- **Lawsuits and Disputes.** If you become involved in a lawsuit or other legal action, the Health Plan may disclose your PHI in response to a court or administrative order, a subpoena, warrant, discovery request, or other forms of lawful due process.

- **Law Enforcement.** The Health Plan may release your PHI if asked to do so by a law enforcement official, for example, to report child abuse, to identify or locate a suspect, material witness, missing person or to report a crime, the crime's location or victims, or the identity, description, or location of the person who committed the crime.

- **Workers' Compensation.** The Health Plan may disclose your PHI to the extent authorized by and to the extent necessary to comply with workers' compensation laws and other similar programs.

- **Military and Veterans.** If you are or become a member of the U.S. armed forces, the Health Plan may release medical information about you as deemed necessary by military command authorities.

- **To Avert Serious Threat to Health or Safety.** The Health Plan may use and disclose your PHI when necessary to prevent a serious threat to your health and safety, or the health and safety of the public or another person.

- **Public Health Risks.** The Health Plan may disclose health information about you for public health activities. These activities include preventing or controlling disease, injury or disability; reporting births and deaths; reporting child abuse or neglect; or reporting reactions to medications or problems with medical products, or to notify people of recalls of products they have been using.

- **Health Oversight Activities.** The Health Plan may disclose your PHI to a health oversight agency for audits, investigations, inspections, and licensure necessary for the government to monitor the health care system and government programs.

- **Research.** Under certain limited circumstances, the Health Plan may use and disclose your PHI for medical research purposes.

- **National Security, Intelligence Activities, and Protective Services.** The Health Plan may release your PHI to authorized federal officials: (1) for intelligence, counterintelligence, and other national security activities authorized by law; and (2) to enable them to provide protection to the members of the U.S. government or foreign heads of state, or to conduct special investigations.

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

- **Coroners, Medical Examiners, and Funeral Directors.** The Health Plan may release your PHI to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or to determine the cause of death. The Health Plan may also release your PHI to a funeral director, as necessary, to carry out his/her responsibilities.

Your Rights Regarding Your Health Information

You have the following rights regarding the health information that the Health Plan maintains about you:

- **Right to Inspect and Copy Your Personal Health Information.** You have the right to inspect and obtain a paper copy your PHI that is maintained in a "designated record set" for so long as the Health Plan maintains your PHI. A "designated record set" includes medical information about eligibility, enrollment, claim and appeal records, and medical and billing records maintained by the Health Plan, but does not include psychotherapy notes, information intended for use in a civil, criminal or administrative proceeding, or information that is otherwise prohibited by law.

  To the extent your PHI is maintained electronically in a designated record set, you also have the right to request a copy of the PHI in a specified electronic form and format. If the requested form and format is not readily producible, the Health Plan will provide the copy in a readable electronic form and format that is agreed to by you and the Health Plan.

  You may request that the paper or electronic copy of your PHI be sent to another entity or person, so long as that request is in writing, signed by you, and clearly identifies the designated entity or person and where to send the copy of the PHI.

  To inspect and obtain a copy of the PHI (in either paper or electronic form) maintained by the Health Plan, submit your request in writing to the Privacy Official. The Health Plan may charge a reasonable, cost-based fee for the cost of copying and/or mailing your request (including the cost of any required supplies).

The Health Plan must act upon your request for access no later than 30 days after receipt. A single, 30-day extension is allowed if the Health Plan is unable to comply by the initial deadline. In limited circumstances, the Health Plan may deny your request to inspect and obtain a copy of your PHI. Generally, if you are denied access to your health information, you will be informed as to the reasons for the denial, and of your right to request a review of the denial.

- **Right to Amend Your Personal Health Information.** If you feel that the health information that the Health Plan has about you is incorrect or incomplete, you may ask the Health Plan to amend it. You have the right to request an amendment for so long as the Health Plan maintains your PHI in a designated record set.

  To request an amendment, send a detailed request in writing to the Privacy Official. You must provide the reason(s) to support your request. The Health Plan may deny your request if you ask the Health Plan to amend health information that was: (1) accurate and complete; (2) not created by the Health Plan, (3) not part of the health information kept by or for the Health Plan; or (4) not information that you would be permitted to inspect and copy. The Health Plan has 60 days after the request is received to act on the request. A single, 30-day extension is allowed if the Health Plan cannot comply by the initial deadline. If the request is denied, in whole or in part, the Health Plan will provide you with a written denial that explains the basis for the denial. You may then submit a written statement disagreeing with the denial and, if permitted under HIPAA, have that statement included with any future disclosures of your PHI.

- **Right to An Accounting of Disclosures.** You have the right to request an "accounting of disclosures" of your PHI. This is a list of disclosures of your PHI that the Health Plan has made to others for the six (6) year period prior to the request, except for those disclosures necessary to carry out treatment, payment, or health care operations, disclosures previously made to you, disclosures that occurred prior to the date on which the accounting is requested, or in certain other situations described under HIPAA.

  To request an accounting of disclosures, submit your request in writing to the Privacy Official. Your request must state a time period, which may not be longer than six (6) years prior to the date the accounting was requested. If the accounting cannot be provided within 60 days, an additional 30 days is allowed if the Health Plan provides you with a written statement of the reasons for the delay and the date by when the accounting will be provided. If you request more than one accounting within a 12-month period, the Health Plan will charge a reasonable, cost-based fee for each subsequent accounting.

- **Right to Request Restrictions.** You have the right to request a restriction on the health information that the Health Plan uses or discloses about you for treatment, payment, or health care operations. You also have the right to request that the Health Plan limits the individuals (for example, family members) to whom the Health Plan discloses health information about you. For example, you could ask that the Health Plan not use or disclose information about a surgical procedure that you had. While the Health Plan will consider your request, it is not required to agree to it. If the Health Plan agrees to the restriction, it will comply with your request until such time as the Health Plan provides written notice to you of its intent to no longer agree to such restriction, or unless such disclosure is required by law.

  To request a restriction or limitation, make your request in writing to the Privacy Official. In your request, you must state: (1) what information you want to limit; (2) whether you want to limit the Health Plan's use, disclosure, or both; and (3) to whom you want the limit(s) to apply.

- **Right to Request Confidential Communications.** You have the right to request that the Health Plan communicate with you about health matters using alternative means or at alternative locations. For example, you can ask that the Health Plan send your explanation of benefits ("EOB") forms about your benefit claims to a specified address. To request confidential communications, make your request in writing to the Privacy Official. The Health Plan will make every attempt to accommodate all reasonable requests. Your request must specify how or where you want to be contacted.

- **State Privacy Rights.** You may have additional privacy rights under state laws, including rights in connection with mental health and psychotherapy reports, pregnancy, HIV/AIDS-related illnesses, and the health treatment of minors.

- **Right to a Paper Copy of this Notice.** You have the right to a paper copy of this Notice upon request. This right applies even if you have previously agreed to accept this Notice electronically. You may write to the Privacy Official to request a written copy of this Notice at any time.

Changes to this Privacy Notice

The Health Plan reserves the right to change this Notice at any time and from time to time, and to make the revised or changed Notice effective for health information that the Health Plan already has about you, as well as any information that the Health Plan may receive in the future. The change to the Notice or the revised Notice will be posted on the Health Plan's web site by the effective date of the change. The revised Notice, or information about the change to the Notice and how to obtain the revised Notice, will be sent to you in the Health Plan's next annual mailing to participants. The revised Notice will be sent electronically if you have consented to receive the Notice electronically.

Complaints

If you believe that your health information privacy rights as described under this Notice have been violated, you may file a written complaint with the Health Plan by contacting the person listed at the address under "Contact Information". You may also file a written complaint directly with the regional office of the U.S. Department of Health and Human Services, Office for Civil Rights. The complaint should generally be filed within 180 days of when the act or omission complained of occurred. Note: You will not be penalized or retaliated against for filing a complaint.

Other Uses and Disclosures of Health Information

The Health Plan is required to receive your written authorization as a condition for:

- Any use or disclosure of your PHI for marketing purposes, except if the communication is in the form of face-to-face communications with you or a promotional gift of nominal value;
- Any use or disclosure of your PHI that is in the form of a sale of PHI; or
- Any use or disclosure of psychotherapy notes, except to carry out certain treatment, payment or health care operations, or as otherwise required by law.

Other uses and disclosures of health information not covered by this Notice or by the laws that apply to the Health Plan will be made only with your written authorization.

If you authorize the Health Plan to use or disclose your PHI, you may revoke the authorization, in writing, at any time. If you revoke your authorization, the Health Plan will no longer use or disclose your PHI for the reasons covered by your written authorization; however, the Health Plan will not reverse any uses or disclosures already made in reliance on your prior authorization.

The Health Plan is prohibited from using or disclosing any of your PHI that is genetic information for underwriting purposes.

Contact Information

To receive more information about the Health Plan's privacy practices or your rights, or if you have any questions about this Notice, please contact the Health Plan at the following address:

Contact Office or Person: Privacy Office
OxyLink Employee Services Center
4500 South 129th East Avenue
Tulsa, Oklahoma 74134

Telephone: (800) 699-6903

Health Plan Names(s):

- Occidental Petroleum Corporation Welfare Plan (Medical, Dental and FSA components)
- Occidental Petroleum Corporation Retiree Medical Plan
- Occidental Petroleum Corporation Retiree Dental Plan
- Occidental Petroleum Corporation Health Promotion Plan
- Occidental Chemical Corporation Medical Plan
- Occidental Chemical Corporation Retiree Medical Plan
- Occidental Chemical Corporation Retiree Dental Plan
- Occidental Chemical Corporation Dental Assistance Plan
- Occidental Chemical Corporation Pretax Premium Plan
- Occidental Chemical Corporation Special Welfare Plan for North Tonawanda Hourly Employees
- Occidental Chemical Corporation Special Welfare Plan for North Tonawanda Salaried Employees
- Blue Cross-Blue Shield Plan for Hourly Employees of Occidental Chemical Corporation at Niagara Falls
- Blue Cross-Blue Shield Plan for Hourly Employees of Occidental Chemical and Plastics Corporation – North Tonawanda
- Group Insurance Plan for Petrolia Hourly Employees
- Group Insurance Plan for Petrolia Hourly Retirees

Copies of this Notice are also available at OxyLink Employee Service Center (800) 699-6903 and online at oxylink.oxy.com.

Effective and Last Updated: January 27, 2015

Appendix F

Complaints Log

Item #	Date Complaint Received	Name of Complainant	Complaint Received By	Nature of Complaint	
1.					
2.					
3.					
4.					
5.					
6.					

Notes:

1. The Plan will log all complaints in writing.
2. Contents of log may be reviewed upon request by any Individual for an Accounting of Disclosures.
3. The Complaint Log will be maintained by the Privacy Officer.

Plan Document Language

(See Privacy Document)

HIPAA Non-Routine Disclosure Log

Item #	Individual/Subject of the ePHI	Date	Specific ePHI Disclosed	Purpose	Mode
1.					
2.					
3.					
4.					
5.					
6.					

Notes:

1. The Plan will log all Non-Routine Disclosures in writing.
2. Contents of log may be reviewed upon request by any Individual for an Accounting of Disclosures.
3. The Non-Routine Disclosure Log will be maintained by the Security Officer.

Appendix I

Training Documentation

See log maintained by Lou Massey.

Appendix J

Breach Notification Log

The breach notification log and related material will be maintained as part of a general Improper Use or Disclosure of PHI log as follows:

Date of Event	Parties Involved	Description of the Event	Description of PHI Involved	Breach Determination and Analysis	CE's efforts to investigate and mitigate potential harm	CE's action to prevent or mitigate reoccurrence	Date individual(s) provided required breach notification (if applicable)