SECTION	Approval date:	
Office Management	Approved by:	
POLICY AND PROCEDURE	Effective date:	
Patient Confidentiality	Revision date:	

POLICY:

Confidentiality of personal medical information is protected according to state and federal guidelines. Patients have the right to privacy for dressing/undressing, physical examination, and medical consultation. Practices are in place to safeguard patient privacy. The patient's private health information shall be maintained secure and confidential in compliance with legal, accrediting and regulatory agency requirements. All member information is regarded as confidential and obtainable only to authorized persons.

PROCEDURE:

A. The primary care provider (PCP) site shall maintain confidentiality of individual patient information. Individual patient conditions or information not discussed in front of other patients or visitors, displayed or left unattended in reception and/or patient flow areas. Patient registration sign-in sheets protect patient's privacy from other patients who may also be checking-in for their appointments. Patient sign-in sheets shall collect only minimal information using no more than one (1) patient identifier such as the patient's name.

B. The PCP site shall ensure that exam rooms and dressing areas safeguard patient's right to privacy.

C. The provider/designee shall ensure that there is a system for the following:
   1. Medical records are available at each encounter and include outpatient, inpatient, referral services, and significant consultations.
   2. Medical records are accessible within the facility, or an approved health record storage facility on the facility premises.

D. Where applicable, electronic record-keeping system procedures are established to ensure patient confidentiality, prevent unauthorized access, authenticate electronic signatures, and maintain upkeep of computer systems. Security protection includes an off-site backup storage system, an image mechanism with the ability to copy documents, a mechanism to ensure that recorded input is unalterable, and file recovery procedures. Confidentiality protection may also include use of encryption, detailed user access controls, transaction logs, idle monitor screen protection and blinded files.

E. The PCP site shall ensure that medical records are not released without written, signed consent from the patient or patient's representative, identifying the specific medical information to be released. The release will indicate to whom released and for what purpose. NOTE: The PCP site shall release and furnish necessary health records without the patient's written, signed consent to coordinate the patient's care with physicians, hospitals, or other health care entities, or to coordinate payment. PCPs shall also provide at no charge to health plans and appropriate state and federal regulators without written, signed consent from the patient, prompt access or upon demand, to medical records or information for quality management or other purposes, including utilization review, audits, reviews of complaints or appeals, HEDIS and other studies within 10 days of the request unless otherwise indicated or as agreed upon.

F. Transmittal of medical records by email shall be encrypted at all times. Transmission of medical records by fax shall include a fax cover page. The fax cover page includes a confidentiality statement which requires the recipient to maintain the information in a safe, confidential and secure manner and provide instructions on what steps to take when the transmittal is received by unintended recipients.

G. The PCP site shall ensure that medical records are retained for a minimum of 10 years following patient encounter.

H. The name of the individual delegated the responsible for securing and maintaining the security of medical records at this location is: _____