SECURE PROVIDER PORTAL: NOTICE OF PHI

AS REQUIRED BY FEDERAL AND STATE LAW, DISTRICT MEDICAL GROUP (DMG) AND ALL OF ITS EMPLOYEES ARE REQUIRED TO ABIDE BY SAFEGUARDS IMPLEMENTED TO RESTRICT THE USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION. THIS NOTICE SERVES AS A REMINDER AND REAFFIRMATION OF YOUR OBLIGATION TO KEEP PROTECTED HEALTH INFORMATION SAFE WHILE USING THE SECURED PROVIDER PORTAL.

THIS NOTICE IS IMPLEMENTED IN ACCORDANCE WITH APPLICABLE DMG POLICIES AND PROCEDURES AND THE REQUIREMENTS OF HIPAA AND OTHER FEDERAL AND STATE LAWS.

PLEASE REVIEW THIS NOTICE CAREFULLY

A. DEFINITIONS

Data: includes electronic information relating to health care services provided to any individual that is made available by or through the Informatics Center, including without limitation Protected Health Information and Personally Identifiable Information.

Health Insurance Portability and Accountability Act of 1996 (HIPAA): provides privacy and security standards to protect patient medical records and other health information provided to health plans, doctors, hospitals and other health care providers.

Informatics Center: means that software, portal, platform, or other electronic medium furnished by DMG to permit electronic access to health information about individuals in connection with one or more health care quality initiative programs administered or sponsored by DMG.

Protected Health Information (PHI): includes any health information and confidential information, whether verbal, written or electronic, created, received, or maintained by DMG. Additionally, PHI relates to the past, present and future physical or mental health of any 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. All patient information including but not limited to claim data, authorization information, and attachments such as medical records and consent forms are all PHI.

Personally Identifiable Information (PII): means information that identifies or may be used to identify an individual, including without limitation first name or first initial and last name in combination with address, driver's license number, credit card number or Social Security number.

B. PRIVACY AND SECURITY SAFEGUARDS

DMG will use appropriate administrative, technical and physical safeguards to protect the confidentiality, integrity, and availability of information and to prevent the use or disclosure of Data other than as permitted or required by applicable Federal or State law. To that end, DMG shall:

(i) Provide appropriate identification and authentication of Authorized Users;

(ii) Provide appropriate access authorization;

(iii) Guard against unauthorized access to Data; and

(iv) Provide appropriate security audit controls and documentation

DMG will apply appropriate sanctions against any provider, subject to DMG's privacy and security policies and procedures, who fails to comply with such policies and procedures. The type and severity of sanctions applied shall be in accordance with DMG's privacy and security policies and procedures. Provider shall make employees, agents, and contractors aware that certain violations may result in notification by DMG to law enforcement officials as well as regulatory, accreditation and licensure organizations.

DMG may, at its discretion, deny access to any provider it has reason to believe accessed, used, or disclosed Data in an inappropriate manner.

C. PROVIDERS' HIPAA OBLIGATIONS

You will be accessing or providing PHI through this Portal. With respect to information accessed through this Portal that constitutes PHI, you shall:

(i) Not use and/or disclose PHI accessed or obtained through this Portal except as permitted under the HIPAA Regulations;

(ii) Use reasonable safeguards to prevent use or disclosure of PHI;

(iii) Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of PHI that Providers create, receive, maintain, or transmit;

(iv) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

(v) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Regulations;

(vi) Ensure that any agent, including a subcontractor, to whom you provide such information agrees to implement reasonable and appropriate safeguards to protect it; and

(vii) Report to DMG any security incident of which you become aware