REGIONAL MEDICAL IMAGING

Main Office
3346 Lennon Road, Flint MI 48507
810.732.1919 PHONE | 810.732.4562 FAX
Villa Linde Pkwy, Flint ■ Fenton
Grand Blanc ■ Davison ■ Lapeer ■ Novi
www.rmipc.net

REGIONAL MEDICAL IMAGING
ROYAL AUTHORIZATION FOR ORDERING PHYSICIANS AND STAFF

We recognize both the need for timely access to accurate information in treating patients and for maintaining the confidentiality, privacy, security, availability, and integrity of such information. Due to the confidential nature of patient records and individually identifiable health, clinical, demographic, insurance, financial, appointment, and related information (Confidential Information), measures must be taken to ensure that Confidential Information may be accessed, used, and disclosed only by authorized users for authorized purposes. Accordingly, you agree to comply with these Terms of Use.

Your Use of Confidential Information.

You will retrieve or attempt to retrieve from the online viewing system (the System) only the specific Confidential Information or other data: that is directly related to the treatment of patients with whom you have a formal treatment relationship; for which you have a legitimate, job-related need to know; or that is directly related to those patients for whom you have been asked to provide medical services consultation.

You will.

1. Protect the confidentiality, privacy, security, availability, and integrity of all Confidential Information.
2. Fully comply with applicable federal, state, and local laws concerning such Confidential Information.
3. Fully comply with our organizational policies and procedures.
4. Not act or fail to act in a manner that may cause us to not be in compliance with any federal, state, or local law or with our policies and procedures.
5. Access, use, and/or disclose Confidential Information only as necessary to provide patient care services.
6. Accurately designate whether you have a formal treatment relationship with the patient.
7. Access, use, and disclose Confidential Information only as needed by you to perform your legitimate duties in connection with your job and patient care responsibilities.
8. Not access or use Confidential Information that you have no legitimate need to know.
9. Not in any way disclose, divulge, copy, release, sell, loan, revise, alter, or destroy any Confidential Information except as properly authorized within the scope of your job responsibilities.
10. Not misuse or carelessly care for or fail to safeguard Confidential Information.
11. Ensure that no programs or devices, such as viruses, worms, Trojan horses, or other forms of malicious or potentially destructive computer code or computer sabotage, will be placed within the System that could disrupt use of the System, or any system, equipment, or software to which the System is interfaced or connected, could destroy, alter, or damage Confidential Information or make data inaccessible or delayed, or could permit any unauthorized personnel to access the System.

REGIONAL MEDICAL IMAGING

Main Office
3346 Lennon Road, Flint MI 48507
810.732.1919 PHONE | 810.732.4562 FAX
Villa Linde Pkwy, Flint ■ Fenton
Grand Blanc ■ Davison ■ Lapeer ■ Novi
www.rmipc.net

Your User ID and Password.

Your User ID and password are your unique identifiers for the System. Your User ID and password are the equivalent of your signature. You are the only person authorized to use your User ID and password. You must not allow others to use your user ID and/or password. You agree to safeguard and will not disclose your User ID and password. You understand that it is your responsibility to log out of the System. You will not, under any circumstances, leave unattended a computer terminal to which you have logged on. You will not, under any circumstances, let another person work under your User ID or Password. You accept responsibility for all activities undertaken using your User ID and password. Passwords should not be written down or posted where they can be seen or easily discovered by others. For instance, passwords should not be posted on terminals or cabinet doors or carried in a case with a laptop. If you have reason to believe the confidentiality of your password has been compromised, you will change your password.

Safeguards.

You will implement and use appropriate administrative, physical, technical, and procedural safeguards to protect the privacy, security, confidentiality, integrity, and availability of Confidential Information entered into, contained on, or transmitted or accessed through the System, to protect against reasonably anticipated threats, and to prevent use or disclosure of such Confidential Information other than as required or permitted by these Terms of Use or required by law. Such safeguards shall comply with federal, state, and local requirements including but not limited to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (the HITECH Act) or their implementing regulations.

Our Right to Monitor.

You understand we have the right to monitor, and to conduct and maintain an audit trail of, access to patient and other Confidential Information and to record the user, date, and patient identification of all access to the System and/or Confidential Information that is electronically maintained. You waive any right to privacy with respect to the use of the System.

Notification.

You immediately will notify us in the event you discover or suspect:

(a) any unauthorized use of or access to the System;
(b) any use or disclosure of Confidential Information contained on the System not permitted by these Terms of Use;
(c) any action or omission that may adversely affect the confidentiality, privacy, security, integrity, or availability of any Confidential Information;
(d) the recognition or introduction of any virus or any malicious or destructive programs;
(e) any actual or suspected breach of these Terms of Use or our protocols, policies, or procedures that affects or may affect Confidential Information entered into contained in, or transmitted or accessed through the System;
(f) any security incident, as defined in HIPAA, of which you become aware; or
(g) a breach, as defined in the HITECH Act, that you may discover.

REGIONAL MEDICAL IMAGING

Main Office
3346 Lennon Road, **Flint** MI 48507
810.732.1919 *PHONE* | 810.732.4562 *FAX*
Villa Linde Pkwy, Flint ■ Fenton
Grand Blanc ■ Davison ■ Lapeer ■ Novi
www.rmipc.net

Access to the System.

We reserve the right, in our sole discretion, to suspend or revoke your access, or any persons or entities access, at any time, on a permanent or temporary basis.

Physician and/or Physician group practice shall immediately notify Regional Medical Imaging when any previously Authorized Person is no longer associated with physician or group practice so that their access may be terminated.

Remedy of Security Incident.

You will cooperate fully with us with respect to any investigation, audit, or other compliance activity related to an actual or suspected breach and will take all reasonable actions, consistent with our recommendations or instructions, to cure the breach and prevent future breaches, and to mitigate the effects of the breach.

No Ownership of Confidential Information.

You understand you have no right or ownership interest in any Confidential Information, the System, or your User ID or password.

Availability of online images cannot be guaranteed due to potential technical difficulties, which may be beyond the control of Regional Medical Imaging. It is essential that any images required for surgery or other invasive procedures be obtained in hard-copy form. It is the responsibility of the physician performing these procedures to obtain CD, paper or film copies of the necessary images in advance.

Practice Name _____

Name of Authorized Employee _____

Signature of Authorized Employee _____

Email _____

Date _____

Revised December 5, 2016