Application to Establish Access to PACS System:

ACCESS REQUIRES THAT YOU:
1) are a physician or are employed by a physician, medical facility, or health organization
2) have an authorized need to access the PACS System (as defined by HIPAA regulations)

Incomplete forms will be considered invalid. Form must be accompanied with the Information Security Agreement. Access requests for more than view only privileges or for individuals without an email account issued by their organization will require a supervisor to complete his/her information and sign the request.

Your Name: _____ Organization _____

Job Title _____ Credentials _____ Phone _____
(MD, DO, RT(R), etc.)

Verification: Last four of SSN _____ Date of Birth _____

Organization-issued Email: _____
NOTE: If you do not have an organization-issued email address, you are required to have your supervisor information and signature.

Access Requested:
☐ View only ☐ View and Export
(Requires signature from your supervisor)

- ✓ You will receive an encrypted email when your account has been activated with your username and sign-on password which you will be required to change at sign-on. Encrypted email will come from Notification@ZixMessageCenter.com. Be sure to check junk and spam folders for the email.

☐ I have read and understand the Information Security Agreement for and my signed copy is attached with this request.

Requestor Signature: _____ Date: _____

Supervisor information required when an organization-issued email is not available AND/ OR the access requested is for more than view only.

Supervisor Name: _____ Title: _____

Organization-issued or
Professional Email: _____ Phone _____

Supervisor Signature: _____ Date: _____

Fax or email your application to the site administrator:
Fax (309) 762-1094 Attn: Compliance Officer
Email: compliance@qcadrad.com

YOU WILL BE NOTIFIED BY MDI WHEN YOUR ACCOUNT IS ACTIVE

To be completed by the site administrator and sent to MDI

☐ Access Approved ☐ Access Denied – Reason for denial: _____

Level of access granted (check all that apply):
☐ View ☐ Export

AIC/Metro Approver: _____ Date: _____

Information Security Agreement

This document has been developed for exclusive or joint use of the following entities:

Advanced Radiology, SC
Advanced Imaging Center, LLC
Metro MRI Center, LP
Medical Data Integration

The agreement covers any access to information created or otherwise maintained by the entities which will be referred to as "the practice" indicating all entities unless otherwise defined.

Patient, financial, and other business-related information in any form, electronic or printed, is a valuable asset and is considered private and sensitive. Employees, physicians, physician office staff, consultants, vendors, contracted agency staff, and students may have access to confidential information in the performance of their duties. Those charged with this responsibility must comply with information confidentiality/ security policies in effect at the practice and its affiliates. This agreement applies regardless of the method of access used.

In consideration of being allowed access to the practice information systems, I, the undersigned, hereby agree to the following provisions:

1. I agree to abide by all present and future confidentiality/ security policies and procedures for the practice and its affiliates. I understand that such policies and procedures are available on the Intranet or may be requested through the practice compliance officer at 309-762-1072.
2. I agree to maintain a unique password, known only to myself, to access the system to read, edit and authenticate data. I understand that my unique password constitutes my electronic signature and that it should be treated as confidential information. I agree not to share my password with any other individual or allow any other individual to use the system once I have accessed it. I understand that I may change my password at any time.
3. I agree to access only information and perform only computer functions as required for the performance of my duties and responsibilities.
4. I agree to close out and/or log off of any application containing PHI in order to prevent unauthorized use of my access.
5. I will contact my supervisor, the practice compliance officer, or Medical Data Integration if I have reason to believe the confidentiality and security of my password has been compromised.
6. I will not disclose any portion of the computerized systems to any unauthorized individuals. This includes, but is not limited to, the design, programming techniques, flow charts, source code, screens, and documentation created by employees, outside resources, or third parties.
7. I will not disclose any portion of the patient's record except to a recipient designated by the patient or to a recipient authorized by the practice who has a "need to know" in order to provide continuing care of the patient.
8. I will not operate or attempt to operate computer equipment without specific authorization.
9. I will not demonstrate the operation of computer equipment or applications to anyone without specific authorization.
10. I understand that applications are available outside of the practice network via various remote access methods, and I agree to abide by the following when accessing the practice computer systems from remote locations:
    a. I will only access the practice computer systems from remote locations if I am authorized to do so.

b. I will use discretion in choosing when and where to access the practice computer systems remotely in order to prevent inadvertent or intentional viewing of displayed or printed information by unauthorized individuals.
c. I will use proper disposal procedures for all printed materials containing confidential or sensitive information.
d. I understand that if I choose to use my personal equipment to access the practice computer systems remotely, it is my responsibility to provide internet connectivity, configure firewall and virus protection appropriately, and to install any necessary software/ hardware. The practice is not responsible if the installation of software necessary for accessing the practice computer systems remotely interferes or disrupts the performance of other software/ hardware on my personal equipment.
e. I understand that by using my personal equipment to access the practice computer systems that my computer is a de facto extension of the practice network while connected, and as such is subject to the same rules and regulations that apply to practice owned equipment.

11. I agree to report any activity which is contrary to the practice policies or the terms of this agreement to my supervisor, the practice compliance officer, or a security administrator.
12. If I will be using a mobile device to access the practice network or network services (through a personally-owned or practice-owned device) that include, but is not limited to, email VPN, or other remote access capabilities, I will allow the practice limited control of my mobile device for the protection of the practice data and its assets. For this context a mobile device is currently identified as a mobile phone tablet or other miniaturized computing system. This limited control can include the enforcement of a password/pin and/or remote wiping of the mobile device in the event of loss or theft or other factors that may present a risk of harm to the practice network, its data, or applications.
13. I agree to comply with all relevant practice compliance policies, including but not limited to the Device and Media Controls – Mobile Devices Policy. I understand that I must sign this Agreement as a precondition to issuance of a computer password for access to the practice network and/or patient information and that failure to comply with the preceding provisions will result in formal disciplinary action, which may include, but will not be limited to, termination of access, termination of employment in the case of employees, termination of agreements in the case of contractors, or revocation of clinical privileges in the case of medical staff members, taken in accordance with applicable medical staff by-laws, rules and regulations.
    - In the event of loss or theft of my device, I agree to the remote wiping of all content on my mobile device, including any personal information I may have stored on the device, such (but not limited to) photos, videos, and other content stored on the hard drive of the device.
    - In the event of an investigation or inquiry by the internal compliance department or the government, or in the event of litigation, I agree to provide the practice and/or its affiliate(s) with access to my device to copy and retain information related to the investigation, inquiry or litigation. I understand that the practice will take reasonable steps to limit access to personal information such as using key word searches to identify relevant material.

I understand that my failure to follow each clause of this agreement will result in suspension and/or revocation of PACS access privileges.

_____ _____
Signature Date

_____ _____
Printed Name Job Title

_____
Company/Department