REFERRAL PORTAL USER AGREEMENT

This Remote Access Users Agreement applies to individuals who are permitted electronic access to St. Joseph's Imaging Associate, PLLC (herein "SJIA") information resources from a remote location including but not limited to SJIA administrative staff, hospital staff, medical staff, affiliates, business associates, board of trustees, physicians, clinical affiliates, vendors, contractors, consultants, students, interns and volunteers.

By signing this document I understand the following:

1.0 Remote access is a privilege and all access to and use of SJIA information resources must be consistent with local, state and federal laws as well as the terms of SJIA policies, goals, standards, and overall mission and values.

2.0 Users are responsible for providing their own Internet access and equipment. SJIA does not service or support end user equipment.

3.0 Secure remote access must be strictly controlled.

4.0 Devices used for remote access must have the following minimum safeguards implemented:

- *4.1. First and foremost, use common sense.*
- *4.2. Do not remotely access medical records from a public place such as a coffee shop, shopping center or airport.*
- *4.3. Configure a strong password to access the device and do not share it with anyone. All activity done while logged on with your ID will be tied to you.*
- *4.5. A firewall must be installed and enabled (if supported).*
- *4.6. Use modern anti-virus software with host intrusion detection/prevention protection enabled. Anti-virus programs must be kept current through automatic updates (i.e. the application and virus definitions), be actively running and configured to run periodic scans.*
- *4.7. All critical security patches must be installed with one month of release. This includes relevant patches for operating systems and all installed applications.*
- *4.10. Physically secure the device when not in use: lock it in a drawer, use a cable lock, and lock your office, etc. Even desktop/tower computers can be stolen; make sure all computers are physically secured.*

6.0 SJIA must be notified immediately after I become aware of any suspected or actual breach of security, intrusion, unauthorized use of information resources or lost/stolen equipment per the Remote Access to Information Resources policy.

7.0 SJIA must be notified when remote access is no longer needed per the Remote Access to Information Resources policy.

8.0 All users are subject to monitoring and auditing of access and compliance with this and other SJIA policies and standards. Users should not have any expectation of privacy while using SJIA resources. Please review the following related policies:

- *8.1. Remote Access to Information Resources*
- *8.2. User ID and Password Management*
- *8.3. Encryption and Decryption*
- *8.4. Sanctions for Privacy & Security Violations*
- *8.5. Security Incident Response & Reporting*

9.0 St. Joseph's reserves the right to terminate remote access privileges at any time.

I, the undersigned, understand that as a condition of conducting business at SJIA, I must abide by the terms of this remote access user agreement. I understand that if I violate these policies, my business with SJIA may be terminated. I also understand that if I do not follow these policies I may be subject to legal action against me by the patient, the facility or any other injured parties.

Business Associate

_____
print name

_____
signature

_____
title

_____
email address

_____
company name

_____
date

Covered Entity (St Joseph's Imaging Associates, PLLC)

_____
signature

_____
date

Lauren Bellotti
Director of Radiology
5100 West Taft Road
Liverpool, NY 13088
(315) 452-2563