

River Parishes Hospital Privileges in Teleradiology

Name: _____

QUALIFICATIONS

To be eligible for core privileges in teleradiology, the applicant must meet the following qualifications:

Properly licensed in the State of Louisiana and credentialed by Virtual Radiologic Consultants and currently working under contract agreement with River Parishes Hospital.

PRIVILEGES INCLUDED IN TELERADIOLOGY CORE
--

Core privileges in Diagnostic Teleradiology includes the reading and interpretation of any diagnostic imaging study that can be sent over a telemedicine link, including but not limited to the following:

- **Computed Tomography (CT) Scans**
- **Ultrasound**
- **Magnetic Resonance (MR) Scans**
- **Nuclear Medicine**
- **Plain Films**

Teleradiology Core:

<input type="checkbox"/> Requested	<input type="checkbox"/> Recommended	<input type="checkbox"/> Not Recommended
<input type="checkbox"/> Recommended with the following modification(s) and reason(s):		

Acknowledgement of practitioner:

I have requested only those specific privileges for which by education, training, current experience, and demonstrated performance I am qualified to perform, and that I wish to exercise at River Parishes Hospital. I hereby attest that the references, reports, records and information are available that verify my qualifications and competency to practice radiology and to perform these requested procedures.

I understand that:

- (a) In exercising any clinical privileges granted, I am constrained by hospital and medical staff policies and rules applicable generally and any applicable to the particular situation.
- (b) Any restriction on the clinical privileges granted to me is waived in an emergency situation and in such a situation my actions are governed by the applicable section of the medical staff bylaws or related documents.

(c) The use of any new or unproven procedure/treatment may be performed only after the regular credentialing process has been completed and the privilege to perform or use said procedure/treatment has been granted to the individual practitioner.

SIGNATURE OF APPLICANT: _____
Date

Department Chair's Recommendation:

I have reviewed the requested clinical privileges and supportive documentation for the above named applicant and recommend action on the privileges as noted above.

SIGNATURE OF APPROVAL: _____
Chairman of Dept of Medicine Date



HEALTH STATEMENT

TO SECTION CHIEF/CHIEF OF STAFF

1. I HEREBY CERTIFY THAT I POSSESS THE NECESSARY MOTOR SKILLS AND CLINICAL EXPERTISE TO JUSTIFY PRIVILEGES IN THOSE AREAS THAT I HAVE REQUESTED, AND I AM FREE OF ANY INFECTIOUS DISEASE.

_____ YES _____ NO

2. IF NO, DO YOU HAVE A PHYSICAL OR MENTAL CONDITION WHICH COULD AFFECT YOUR ABILITY TO EXERCISE THE CLINICAL PRIVILEGES REQUESTED OR WOULD REQUIRE AN ACCOMMODATION IN ORDER FOR YOU TO EXERCISE THE PRIVILEGES REQUESTED SAFELY AND COMPETENTLY? TO ANSWER THIS QUESTION APPROPRIATELY, PLEASE REPORT ANY CONDITION WHICH IS INFECTIOUS, WHICH AFFECTS MOTOR SKILLS, COGNITIVE ABILITY OR JUDGMENT, OR WHICH MAY ADVERSELY AFFECT YOUR ABILITY TO CARE FOR PATIENTS OR TO INTERACT APPROPRIATELY WITH OTHER CAREGIVERS.

_____ YES _____ NO

If yes, please explain:

3. HAVE YOU TESTED POSITIVE FOR THE TUBERCULIN SKIN TEST?

_____ YES _____ NO

If yes, please give date of positive skin test. _____
If no, when was your last PPD test? _____

REGARDLESS OF HOW THIS QUESTION IS ANSWERED, THE APPLICATION WILL BE PROCESSED IN THE USUAL AND CUSTOMARY MANNER. IF YOU HAVE ANSWERED THIS QUESTION AFFIRMATIVELY AND ARE FOUND TO BE PROFESSIONALLY QUALIFIED FOR MEDICAL STAFF APPOINTMENT AND ABLE TO PERFORM THE CLINICAL PRIVILEGES REQUESTED, YOU WILL BE GIVEN AN OPPORTUNITY TO MEET WITH THE EXECUTIVE COMMITTEE TO DETERMINE WHAT ACCOMMODATIONS, IF ANY, ARE NECESSARY TO ALLOW YOU TO PRACTICE SAFELY.

SIGNATURE OF APPLICANT

DATE

3. _____
Employer Name _____ **City, State** _____ **Phone Number** _____

Dates: To / From _____ **Job Title** _____ **Reason for Leaving** _____

Education (use additional page if needed)

_____ **Institute Name** _____ **City, State** _____

Dates Attended _____ **Graduated?** Yes No _____ **Degree Earned** _____

_____ **Institute Name** _____ **City, State** _____

Dates Attended _____ **Graduated?** Yes No _____ **Degree Earned** _____

Please provide three (3) Professional References

1. _____
Reference Name _____ **City, State** _____ **Phone Number** _____
 2. _____
Reference Name _____ **City, State** _____ **Phone Number** _____
 3. _____
Reference Name _____ **City, State** _____ **Phone Number** _____

Have you ever been convicted of a crime? No Yes If yes, please provide city and state of conviction and details of conviction.

FAIR CREDIT REPORTING ACT NOTICE:

In accordance with the Fair Credit Reporting Act (FCRA, Public Law 91-508, Title VI), this information may only be used to verify a statement(s) made by an individual in connection with legitimate business needs. The depth of information available varies from state to state. Status of updates are available on request. Although every effort has been made to assure accuracy, General Information Services, Inc. cannot act as guarantor of information accuracy or completeness. Final verification of an individual's identity and proper use of report contents are the user's responsibility. General Information Services, Inc.'s policy requires purchasers of these reports to have signed a Service Agreement. This assures General Information Services, Inc. that users are familiar with and will abide by their obligations, as stated in the **FCRA**, to the individuals named in these reports. If information contained in this report is responsible for the suspension or termination of an employee or the application process, have the Candidate/employee contact General Information Services, Inc.

NOTICE TO CALIFORNIA CANDIDATES

You have a right to obtain a copy of any consumer report or investigative consumer report obtained by LIFEPOINT HOSPITALS, INC by checking the box provided below. The report will be provided to you within three (3) business days after we receive the requested reports related to the matter investigated.

I request to receive a free copy of this report by checking this box.

Under section 1786.22 of the California Civil Code, you may view the file maintained on you by GIS during normal business hours. You may also obtain a copy of this file upon submitting proper identification and paying the costs of duplication services, by appearing at GIS in person or by mail. You may also receive a summary of the file by telephone. The agency is required to have personnel available to explain your file to you and the agency must explain to you any coded information appearing in your file. If you appear in person, a person of your choice may accompany you, provided that this person furnishes proper identification.

DEPARTMENT: Information Technology & Services	POLICY DESCRIPTION: Confidentiality and Security Agreements
PAGE: 1 of 4	REPLACES POLICY DATED: 3/19/01, 1/20/03 LifePoint Policy: IS.AA.013, 1/20/03 (retired)
APPROVED: 6/28/10	RETIRED:
EFFECTIVE DATE: 6/29/10	REFERENCE NUMBER: LPNT.IS.SEC.005

SCOPE: All facilities affiliated with the Company including, but not limited to, hospitals, ambulatory surgery centers, home health agencies, physician practices, and all corporate departments and divisions.

PURPOSE:

To provide awareness of the importance of information security and confidentiality and to authorize and require agreements with workforce members, and external entities to protect Company information resources, including confidential patient information.

POLICY:

A. Information Confidentiality and Security Agreements with Individuals

1. All Company employees and other individuals granted access to Company and/or patient protected health information (PHI) must sign and abide by the Confidentiality and Security Agreement (Agreement). The Agreement acknowledges specific responsibilities the individual has in relation to information security and the protection of sensitive information, including confidential patient information, from unauthorized disclosure.
2. Entities not owned and individuals not employed by the Company or an affiliate of the Company shall sign an Agreement if (i) the entity and individual provides services on premises owned or operated by the Company or an affiliate of the Company; (ii) the entity or individual has remote access to the Company's or its affiliates' information systems; or (iii) the entity or individual has access to Company's confidential information or PHI. All contracts for these services must contain enforcement provisions that are consistent with the Company's or its affiliates' disciplinary policies.
3. Any changes to the Agreement must be reviewed and approved in advance by Corporate Information Technology & Services (IT&S) and Legal Counsel.

B. Business Contracts with Business Partners. Relationships with an external entity involving access to Company information systems or the exchange, transmission, storage and maintenance or use of sensitive Company information require a formal contract including provisions to protect the confidentiality and security of Company information and/or systems in accordance with federal HIPAA Security Requirements.

C. Sanctions. Violations of this policy could lead to disciplinary measures up to and including

DEPARTMENT: Information Technology & Services	POLICY DESCRIPTION: Confidentiality and Security Agreements
PAGE: 2 of 4	REPLACES POLICY DATED: 3/19/01, 1/20/03 LifePoint Policy: IS.AA.013, 1/20/03 (retired)
APPROVED: 6/28/10	RETIRED:
EFFECTIVE DATE: 6/29/10	REFERENCE NUMBER: LPNT.IS.SEC.005

termination of employment or business relationship. Suspected violations of this policy are to be handled in accordance with the *Information Security Policy, LPNT.IS.SEC.001*, *Protected Health Information Incident Response, HIPAA.GEN.007* and the Discipline section of the Code of Conduct. Violations may be reported in accordance with the *HIPAA Complaint Process & Disciplinary Actions Policy, HIPAA.GEN.003* located on the Compliance SharePoint site. In addition, violations may be reported to the Ethics Line at 1-877-508-LIFE.

- D. **Policy Exceptions.** Exceptions to Information Security Policy are to be submitted to the Corporate IT&S Information Security Policy key contact for review and approval.

PROCEDURE:

- A. The Confidentiality & Security Agreement form will be posted and maintained by Corporate IT&S on the Company Intranet located under Security.
- B. Each Company and Company affiliate employee and member of the workforce (e.g. volunteers, contract labor, etc.) must sign the Agreement at the time of employment. The completed Agreement will be maintained in the individual's personnel folder.
- C. Each physician and allied health professional must sign the Agreement at the time he or she is appointed to a facility's medical staff. Completed Agreements will be maintained in the individual's credentials file.
- D. Non-employed physician office staff must sign the Agreement at the time information system access is granted. Completed Agreements must be maintained in a central location by the Physician Support Coordinator or individual with a similar role in the business unit.

Representatives of vendors and other external entities must sign the Agreement at the time information access is granted. Completed Agreements must be maintained in the individual contract folder or system (e.g., ShiftWise) by Facility personnel.

REFERENCES:

Government

American Recovery and Reinvestment Act of 2009, Title XIII, Health Information Technology, Subtitle D: Privacy
 Medical Records Confidentiality Act of 1995 (MRCA)
 Health Insurance Portability and Accountability Act, Security Standards for the Protection of Electronic Protected Health Information, 45 CFR Parts 160, 162, and 164

DEPARTMENT: Information Technology & Services	POLICY DESCRIPTION: Confidentiality and Security Agreements
PAGE: 3 of 4	REPLACES POLICY DATED: 3/19/01, 1/20/03 LifePoint Policy: IS.AA.013, 1/20/03 (retired)
APPROVED: 6/28/10	RETIRED:
EFFECTIVE DATE: 6/29/10	REFERENCE NUMBER: LPNT.IS.SEC.005

LifePoint

Information Security – Program Requirements – LPNT.IS.SEC.001
 HIPAA Complaint Process & Disciplinary Actions – HIPAA.GEN.003
 Protected Health Information Incident Response – HIPAA.GEN.007
 Patient Right to Access – HIPAA.PRI.006

HCA

Information Security – Program Requirements, IS.SEC.001
 Information Security - Confidentiality and Security Agreements Policy, IS.SEC.005

Confidentiality and Security Agreement

I understand that the facility or business entity named below (the “Company”) in which or for whom I work, volunteer or provide services, or with whom the entity (*e.g.*, physician practice) for which I work has a relationship (contractual or otherwise) involving the exchange of health information (the “Company”), has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients’ health information. Additionally, the Company must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning, communications, computer systems and management information (collectively, with individually identifiable health information and protected health information, “Confidential Information”).

In the course of my employment / assignment at the Company, I understand that I may come into the possession of this type of Confidential Information. I will not use company systems to access patient information if it is not necessary to perform my job related duties. This includes NOT accessing my own health information or that of my child or person’s for which I am personal representative via the company systems. The Company’s Privacy and Security Policies available on the Company intranet (on the Security Page) and the internet (under

1. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it.
2. I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized.
3. I will not discuss confidential information where others can overhear the conversation, even if the patient’s name is not used. I will make every reasonable attempt to refrain from practices that might lend itself to unintended breach of patient confidentiality.
4. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information.
5. I agree that my obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with the Company.
6. Upon termination, I will immediately return any documents or media containing Confidential Information to the Company.
7. I understand that I have no right to any ownership interest in any information accessed or created by me during my relationship with the Company.
8. I will act in the best interest of the Company and in accordance with its Code of Conduct at all times during my relationship with the Company.
9. I understand that violation of this Agreement may result in disciplinary action, up to and including termination of employment, suspension and loss of privileges, and/or termination of authorization to work within the Company, in accordance with the Company’s policies.
10. I will only access or use systems or devices I am officially authorized to access, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.
11. I understand that I should have no expectation of privacy when using Company information systems. The Company may log, access, review, and otherwise utilize information stored on or passing through its systems, including e-mail, in order to manage systems and enforce security.
12. I will practice good workstation security measures such as locking up electronic media devices when not in use, using screen savers with activated passwords appropriately, and position screens away from public view.
13. I will practice secure electronic communications by transmitting Confidential Information only to authorized entities, in accordance with approved security standards.
14. I will:
 - a. Use only my officially assigned User-ID and password (and/or token (*e.g.*, SecurID card)).
 - b. Use only approved licensed software.
 - c. Use a device with virus protection software.
15. I will never:
 - d. Share/disclose user-IDs, passwords or tokens.
 - e. Use tools or techniques to break/exploit security measures.
 - f. Connect to unauthorized networks through the systems or devices.
16. I will notify my manager, Local Security Coordinator (LSC), or appropriate Information Services person if my password has been seen, disclosed, or otherwise compromised, and will report activity that violates this agreement, privacy and security policies, or any other incident that could have any adverse impact on Confidential Information.

The following statements apply to physicians using any Company systems containing patient identifiable health information (*e.g.* HMS, Meditech, eCW):

17. I will only access software systems to review patient records or Company information when I have a business need to know, as well as any necessary consent. By accessing a patient’s record or Company information, I am affirmatively representing to the Company at the time of each access that I have the requisite business need to know and appropriate consent, and the Company may rely on that representation in granting such access to me
18. I will accept full responsibility for the actions of my employees who may access the Company software systems and Confidential Information.
19. I have no intention of varying the volume or value of referrals I make to the Company in exchange for Internet access service or for access to any other Company information.
20. I have not agreed, in writing or otherwise, to accept Internet access in exchange for the referral to the Company of any patients or other business.
21. I understand that the Company may decide at any time without notice to no longer provide access to any systems to physicians on the medical staff unless other contracts or agreements state otherwise. I understand that if I am no longer a member of the facility’s medical staff, I may no longer use the facility’s equipment to access the Internet.

Signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above.

Employee/Consultant/Vendor/Office Staff/ Physician Signature	Facility Name and COID NNRH	Date
Employee/Consultant/Vendor/Office Staff/ Physician Printed Name	Business Entity Name	

CONTINUING EDUCATION

1. Do you wish to request additional privileges in recognition of education enhancement? _____ Yes _____ No

2. If yes, please list these on the enclosed delineation of privilege request form.

STATEMENT OF CONTINUING MEDICAL EDUCATION ATTESTATION

The Louisiana State Board of Medical Examiners requires no less than 20 hours of Category I CMEs each year for license renewal. I hereby certify that within the past two years I have completed at least the minimum number of hours of continuing education credits required by the board through which I am licensed, and have participated in all performance improvement activities as specified by the hospital(s) at which I have privileges. If audited, I will be able to provide documentation of the seminars or courses attended. I recognize that failure to produce documentation upon request will jeopardize my membership on the medical staff.

Provider Name (Printed)

Provider Signature

Date