INFORMATION SYSTEMS ACCESS REQUEST FORM

(1) Applicant Last Name (print)	(2) Applicant First Name (print)	(3) MI or "NA"

(4) Applicant Phone Number (and Extension)	(5) Date of Birth	(6) Social Security Number

(7) Department #	(8) Department Name	(9) Job Function/Title

(10) If applicant is replacing a terminated employee, please list the terminated employee's name	(11) List another Employee who has the same Job Function as the Applicant

Complete this section only if applicant is NOT an employee of River Park Hospital

(12) ☐Contractor ☐Vendor ☐Physician Office **(Physician/Group or Company name & address)**	(13) **For Contractors and Vendors only** – Enter the End date of engagement or contract.

SELECT THE SYSTEMS THE USER NEEDS ACCESS TO

- ☐ Business Objects
- ☐ Collections-Artiva
- ☐ Document Direct / View Direct
- ☐ EDM
- ☐ Full Internet Access
- ☐ Kronos iSeries
- ☐ Lawson
- ☐ Medibuy / GHX
- ☐ Meditech
- ☐ OnBase - PAS Imaging
- ☐ Outlook Email
- ☐ PACS – Digital Xrays
- ☐ PC-Computer Account
- ☐ Remote Connectivity (VPN)
- ☐ SMART
- ☐ SSI
- ☐ Vista Report Viewer
- ☐ VPOM - Data Processing Rpts

HOST Applications

U	I	Application
		Accounts Payable
		Budget
		Corporate Projection Summary
		Departmental Operations Support
		Facility Override
		Fixed Assets
		Functional Department
		Funds Management
		General Accounting
		General Ledger
		Management Reporting Reviews
		Occurrence Reporting
		Operating Statistics
		Patient Accounting - Billing Inquiry
		Patient Accounting - Custom Reporting
		Patient Accounting - Discrepancy Rpting
		Patient Accounting - Inst Contract Sys
		Patient Accounting – Logging

Please indicate whether **U**pdate or **I**nquiry access should be granted.

U	I	Application
		Patient Accounting – Master Files
		Patient Accounting - Online Cashiering
		Patient Accounting - Pricing Options
		Pay/Ben/hrs - Col/HCA Benefits
		Pay/Ben/hrs - Global Employee Maint
		Pay/Ben/hrs - Human Resources
		Pay/Ben/hrs - On-line Payroll
		PBS Billing Requests
		Provider Credentialing
		QMIRS Statistics Maintenance
		SAIS
		Statcap - Daily Operating Summary
		Transaction Maintenance
		View Direct Report Viewing
		Web Tools & Apps
		SMA: Standard Mth End Accruals
		IBIP: Internet Bill Inquiry/Pymt
		Internal Audit – Self Audit Web Site

ANY OTHER SYSTEM : _____

_____

(14) Manager's Signature	(15) Date	(16) Phone

(17) Hospital Local Security Coordinator Signature	(18) Date	(19) Phone

Please FAX completed form to: 931-815-4620. For questions, please call: 931-815-4116, 4404, or 4105

Confidentiality and Security Agreement

I understand that the facility or business entity (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 patient identifiable 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 access and use this information only when it is necessary to perform my job related duties in accordance with the Company's Privacy and Security Policies, which are available on the Company intranet (on the Security Page) and the internet (under Ethics & Compliance). I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information.

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. It is not acceptable to discuss Confidential Information even if the patient's name is not used.
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 diskettes 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:
    a. Share/disclose user-IDs, passwords or tokens.
    b. Use tools or techniques to break/exploit security measures.
    c. 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 Company systems containing patient identifiable health information (e.g. CPCS/Meditech):

17. I will only access software systems to review patient records when I have that patient's consent to do so. By accessing a patient's record, I am affirmatively representing to the Company at the time of each access that I have the requisite patient consent to do so, and the Company may rely on that representation in granting such access to me.
18. I will insure that only appropriate personnel in my office will access the Company software systems and Confidential Information and I will annually train such personnel on issues related to patient confidentiality and access.
19. I will accept full responsibility for the actions of my employees who may access the Company software systems and Confidential Information.

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 **River Park Hospital / 13100**	Date
Employee/Consultant/Vendor/Office Staff/Physician Printed Name	Business Entity Name	