

## HCA Mountain Division

IT&S Security Access Request Form (Non-Physicians)  
 Fax back to 1-877-253-4812 when completed.

Questions? Call IT&S Service Desk

This information will be kept confidential to the extent allowable by law.

**Please be sure to attach a SIGNED Confidentiality Agreement found on page 3 of this document.**

Employee     
  Student/Agency/Temporary Employee     
  Vendor



*If you are a student/agency/temporary employee or a vendor, please complete the following:*

**Contracting Company Name:** \_\_\_\_\_ **Contract Expiration Date:** \_\_\_\_/\_\_\_\_/\_\_\_\_

**YOU MUST USE YOUR LEGAL FIRST AND LAST NAME ON THIS FORM.** Please note any alternate first names you prefer. The name below must match the name on your professional license if you have one. **\*\*PLEASE PRINT LEGIBLY\*\***

Name: \_\_\_\_\_ Universal ID: \_\_\_\_\_ Job Title: \_\_\_\_\_  
 (First MI Last )

Social Security Number: \_\_\_\_\_ Date of Birth: \_\_\_\_/\_\_\_\_/\_\_\_\_ Business Phone#: \_\_\_\_\_

Facility/COID: \_\_\_\_\_ Dept #: \_\_\_\_\_ Dept Name: \_\_\_\_\_

Start Date: \_\_\_\_/\_\_\_\_/\_\_\_\_ Status Change Date: \_\_\_\_/\_\_\_\_/\_\_\_\_ Status Change: \_\_\_\_\_ **NEED BY DATE:** \_\_\_\_/\_\_\_\_/\_\_\_\_

System	Additional Information		
<input type="checkbox"/> Network <input type="checkbox"/> Add Microsoft Outlook			
<input type="checkbox"/> Remote Access	What systems will you need to access remotely?		
<input type="checkbox"/> Vocera	Department:	Group/Role:	
<input type="checkbox"/> CPCS/Meditech <input type="checkbox"/> Add MOX	Role or Like User:	Credentials:	Facilities:
<input type="checkbox"/> PACS	Access type: <input type="checkbox"/> Physician <input type="checkbox"/> Radiologist <input type="checkbox"/> Nurse <input type="checkbox"/> Technician <input type="checkbox"/> Clerical <input type="checkbox"/> Super User		
<input type="checkbox"/> QS	Access type: <input type="checkbox"/> Physician <input type="checkbox"/> Nurse <input type="checkbox"/> Student <input type="checkbox"/> OB		
<input type="checkbox"/> TraceMaster/GE MUSE	<input type="checkbox"/> View, Print, and Fax [RefPhys]	If additional permission is required, please contact the EKG manager at your hospital.	
<input type="checkbox"/> Host (Oasis) <input type="checkbox"/> PLUS Productivity System <input type="checkbox"/> Document Direct/ View Direct	Please fill out section I on page 2 and/or setup like user: _____		**CFO/Controller Approval Signature Required on page 2 for HOST access.
	Security Level:		
	Department Numbers:		
<input type="checkbox"/> Smart	<input type="checkbox"/> Materials Mgmt <input type="checkbox"/> Accounts Payable    Job Role: _____		
<input type="checkbox"/> GHX Catalyst/Medibuy	Limit \$:	Default Dept. #:	Approver:
<input type="checkbox"/> Corporate Express EWay	Spending Limit \$:	Dept. Numbers:	Approver:
<input type="checkbox"/> Kronos - i Series	Dept. Numbers:		
<input type="checkbox"/> Other	Please specify:		

Authorizing Person's Signature: \_\_\_\_\_

Authorizing Person's Printed Name: \_\_\_\_\_

Date of Signature: \_\_\_\_/\_\_\_\_/\_\_\_\_ Phone Number: \_\_\_\_\_ Authorizing Person's 3/4ID: \_\_\_\_\_

**Section I**

**ONLY REQUIRED FOR HOST**

Levels: I = Inquiry U = Update

**\*\*Approval Signature Required Below\*\***

**On-Line Applications Access Authorization** (Indicate Level & Check Box to Request)

Lvl	Application	Lvl	Application
	<input type="checkbox"/> Accounts Payable		<input type="checkbox"/> Patient Accounting – Master Files
	<input type="checkbox"/> Budget		<input type="checkbox"/> Patient Accounting - Online Cashiering
	<input type="checkbox"/> Budget Access		<input type="checkbox"/> Patient Accounting - Pricing Options
	<input type="checkbox"/> Central Business Systems		<input type="checkbox"/> Pay/Ben/hrs - Col/HCA Benefits
	<input type="checkbox"/> Company Master Report Entity		<input type="checkbox"/> Pay/Ben/hrs- Global Employee Maintenance
	<input type="checkbox"/> Corporate Projection Summary		<input type="checkbox"/> Pay/Ben/hrs - Human Resources
	<input type="checkbox"/> Customer Hardware Support		<input type="checkbox"/> Pay/Ben/hrs - On-line Payroll
	<input type="checkbox"/> Departmental Operations Support		<input type="checkbox"/> PBS Billing Requests
	<input type="checkbox"/> Facility Override Inquiry		<input type="checkbox"/> Provider Credentialing
	<input type="checkbox"/> Facility Override Selection		<input type="checkbox"/> QMIRS Statistics Maintenance
	<input type="checkbox"/> Facility Profile Inquiry		<input type="checkbox"/> SAIS
	<input type="checkbox"/> Fixed Assets		<input type="checkbox"/> Service Costing
	<input type="checkbox"/> Functional Department		<input type="checkbox"/> Statcap - Daily Operating Summary
	<input type="checkbox"/> Funds Management		<input type="checkbox"/> Supplier Management
	<input type="checkbox"/> General Ledger		<input type="checkbox"/> Transaction Maintenance
	<input type="checkbox"/> Information Management Analysis		<input type="checkbox"/> User Override Inquiry
	<input type="checkbox"/> Management Reporting Review		<input type="checkbox"/> User Override Selection
	<input type="checkbox"/> Occurrence Reporting		<input type="checkbox"/> User Profile Inquiry
	<input type="checkbox"/> Operating Statistics		<input type="checkbox"/> View Direct Report Viewing
	<input type="checkbox"/> Patient Accounting – Billing Inquiry		<b>**Web Tools Apps **</b> <input type="checkbox"/> IBIP <input type="checkbox"/> PACF
	<input type="checkbox"/> Patient Accounting – Custom Reporting		<input type="checkbox"/> Patient Accounting –Discrepancy Reporting
	<input type="checkbox"/> Patient Accounting - Inst Contract System		<input type="checkbox"/> Standard M/E Accruals
	<input type="checkbox"/> Patient Accounting - Logging		<input type="checkbox"/> Internal Web Audit
			<input type="checkbox"/> Plus Dept # List: _____

CFO/Controller’s Authorizing Signature: \_\_\_\_\_

Printed Name: \_\_\_\_\_ Date of Signature: \_\_\_\_/\_\_\_\_/\_\_\_\_

**Section II**

**ONLY REQUIRED FOR DOCUMENT DIRECT/VIEW DIRECT**

**View Direct / Document-Report Access**

New User  Update with information below  Delete Access

Remote Printer ID: R\_\_\_\_\_ COID(s): \_\_\_\_\_

Report Groups for User Access (for all COIDs listed above):

- |  |  |
|--|--|
| <input type="checkbox"/> AP/RC/FM                          | <input type="checkbox"/> PAAGNY (Agency)                         |
| <input type="checkbox"/> BS*                               | <input type="checkbox"/> PAAR/PACUST/PAREV (AR)                  |
| <input type="checkbox"/> CM*(Facility Core Coding)         | <input type="checkbox"/> PABDBT (Bad Debt)                       |
| <input type="checkbox"/> EP (Electronic Processing)        | <input type="checkbox"/> PABILL (Billing)                        |
| <input type="checkbox"/> GL* (General Ledger)              | <input type="checkbox"/> PACENS /PAPREA (Census)                 |
| <input type="checkbox"/> QM*(Qmirs)                        | <input type="checkbox"/> PACOLL /PACPAS (Collections)            |
| <input type="checkbox"/> RM*(RM34641 & RM34741 only)       | <input type="checkbox"/> PACONT/PADMR (Balancing)                |
| <input type="checkbox"/> SN* (Senior Friend)               | <input type="checkbox"/> PACPAJ (Cashiering / Ancillary charge)  |
| <input type="checkbox"/> TS* (Facility Trending/Screening) | <input type="checkbox"/> LDG1, LDG2, AR04 (Ledger — Pt Accounts) |
| <input type="checkbox"/> S* (Security Information)         | <input type="checkbox"/> LGLOG (Logging)                         |
| <input type="checkbox"/> HR* (Flex (FL) & Personnel (PS))  | <input type="checkbox"/> PAPME (Master File)                     |
| <input type="checkbox"/> PR* (Field Payroll)               |  |
| <input type="checkbox"/> Plus*                             |  |

**\*\*IMPORTANT\*\***

It is the responsibility of the Local Security Coordinator (LSC) to approve the report groups being granted access. As an appointee of the CFO or controller it is your responsibility to assure security.

## 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 information, or any information that contains Social Security numbers, health insurance claim numbers, passwords, PINs, encryption keys, credit card or other financial account numbers (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 and in the scope of 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. Disclose passwords, PINs, or access codes.
  - 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.
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.

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	Date
Employee/Consultant/Vendor/Office Staff/Physician Printed Name	Business Entity Name	