# North Florida Division
# Security Access Form Completion Instructions

## Office Staff Requesting Access

1. Complete all required fields on the Security Access Form
2. Please type all of the information in each field
3. Read Confidentiality and Security Agreement (CSA)
3. Print Form
4. Sign and date CSA form

**Completed Forms can either be Faxed or Emailed to the corresponding hospital below**

| Hospital | Fax Number | Email Address |
|---|---|---|
| Capital Regional Medical Center | 1-833-219-1096 | CRMC.POSAccess@HCAHealthcare.com |
| Fort Walton Beach Medical Center | 1-833-219-1097 | FWMC.POSAccess@HCAHealthcare.com |
| Gulf Coast Regional Medical Center | 1-833-250-8287 | GCMC.POSAccess@HCAHealthcare.com |
| Twin Cities Hospital | 1-833-219-1098 | TCHO.POSAccess@HCAHealthcare.com |
| West Florida Hospital | 1-844-620-8147 | WFLH.POSAccess@HCAHealthcare.com |
| Lake City Medical Center | 1-833-219-1093 | LCMC.POSAccess@HCAHealthcare.com |
| North Florida Regional Medical Center | 1-844-808-9028 | NFRM.POSAccess@HCAHealthcare.com |
| Ocala/West Marion | 1-844-449-3676 | OCAL.WCHPOSAccess@HCAHealthcare.com |
| Putnam Community Medical Center | 1-833-783-8296 | PCMC.POSAccess@HCAHealthcare.com |
| Central Florida Regional Hospital | 1-844-449-3678 | CFRH.POSAccess@HCAHealthcare.com |
| Osceola Regional Medical Center | 1-844-861-1812 | ORMC.POSAccess@HCAHealthcare.com |
| Oviedo Medical Center | 1-844-425-2327 | OMCT.POSAccess@HCAHealthcare.com |
| Poinciana Medical Center | 1-833-239-2391 | PMC.POSAccess@HCAHealthcare.com |

Please allow 7-10 business days for processing

For questions, please send an email associated with corresponding hospital

24/7 Service Desk 1-888-252-3397

# Non-Privileged PROVIDERS & OFFICE STAFF

**North Florida Division** IT&S SECURITY ACCESS REQUEST FORM

**ALL INFORMATION REQUESTED ON THIS FORM IS REQUIRED**

**Please be sure to sign the Confidentiality and Security Agreement found on pages 2-3 of this document. QUESTIONS? Call the IT&S Service Desk 1-888-252-3397**

## PRACTICE INFORMATION

Practice / Company Name: _____

Company Address: _____ _____ _____ _____
Street City State Zip

Business Phone #:_____ Business Fax #:_____

Providers at this Practice/Company/Location: _____

Office Manager (full name): _____ Office Manager Email: _____

## PERSONAL INFORMATION

Name: _____ Professional Title: _____
Last First MI

Home Address: _____ _____ _____ _____
Street City State Zip

Email Address: _____ Personal Cell #:_____

Date of Birth: _____ / _____ / _____ NPI Number (Providers only):_____

## Access Information

☐ **New** ☐ **Change** ☐ **Reactivation**

- ☐ Capital Regional Medical Center
- ☐ Central Florida Regional Hospital
- ☐ Gulf Coast Regional Medical Center
- ☐ Ft Walton Regional Medical Center
- ☐ Lake City Medical Center
- ☐ North Florida Regional Medical Center
- ☐ Ocala Regional Medical Center / West Marion
- ☐ Osceola Regional Medical Center
- ☐ Oviedo Medical Center
- ☐ Poinciana Medical Center
- ☐ Putnam Community Medical Center
- ☐ Twin Cities Hospital
- ☐ West Florida Hospital

**Setup access like my co-worker**: _____

**PLEASE NOTE:** HCA Medical Staff Office is required to authorize all provider access requests.
**Physicians are required to authorize any office staff requests by signing page 3.**

# Confidentiality and Security Agreement

***Note: this form to be used for non-employed physicians, providers and their non-HCA-employed staff.***

I understand that the HCA affiliated facility or business entity (the "Company") at which I have privileges or for which I work, volunteer or provide services manages health information as part of its mission to treat patients. Further, I understand that 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, credentialing, intellectual property, 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 affiliation or employment with 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 or Company provided systems.

### General Rules

1. I will act in accordance with the Company's Code of Conduct at all times during my relationship with the Company.
2. 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 email, in order to manage systems and enforce security.
3. 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.
4. 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.
5. 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.
6. 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.

### Protecting Confidential Information

7. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it. I will not take media or documents containing Confidential Information home with me unless specifically authorized to do so as part of my job.
8. I will not publish or disclose any Confidential Information to others using personal email, or to any Internet sites, or through Internet blogs or sites such as Facebook or Twitter. I will only use such communication methods when explicitly authorized to do so in support of Company business and within the permitted uses of Confidential Information as governed by regulations such as HIPAA.
9. I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized. I will only reuse or destroy media in accordance with Company Information Security Standards.
10. In the course of treating patients, I may need to orally communicate health information to or about patients. While I understand that my first priority is treating patients, I will take reasonable safeguards to protect conversations from unauthorized listeners. Such safeguards include, but are not limited to: lowering my voice or using private rooms or areas where available.
11. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information.
12. I will secure electronic communications by transmitting Confidential Information only to authorized entities, in accordance with industry-approved security standards, such as encryption.

### Following Appropriate Access

13. I will only access or use systems or devices I am officially authorized to access, will only do so for the purpose of delivery of medical services at this facility, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.
14. 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.
15. I will insure that only appropriate personnel in my office, who have been through a screening process, will access the Company software systems and Confidential Information and I will annually train such personnel on issues related to patient confidentiality and access.
16. I will accept full responsibility for the actions of my employees who may access the Company software systems and Confidential Information.

**PLEASE NOTE:** HCA Medical Staff Office is required to authorize all provider access requests.
**Physicians are required to authorize any office staff requests by signing page 3.**

17. I agree that if I, or my staff, stores Confidential Information on non-Company media or devices (*e.g*., PDAs, laptops) or transmits data outside of the Company network, that the data then becomes my sole responsibility to protect according to federal regulations, and I will take full accountability for any data loss or breach.

**Doing My Part – Personal Security**

18. I understand that I will be assigned a unique identifier ( *e.g.*, 3-4 User ID) to track my access and use of Confidential Information and that the identifier is associated with my personal data provided as part of the initial and/or periodic credentialing and/or employment verification processes.
19. I will ensure that members of my office staff use a unique identifier to access Confidential Information.
20. 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.
21. I will never:
    a. Disclose passwords, PINs, or access codes.
    b. Allow another individual to use my digital identity (e.g., 3-4 User ID) to access, modify, or delete data and/or use a computer system.
    c. Use tools or techniques to break/exploit security measures.
    d. Connect unauthorized systems or devices to the Company network.
22. I will practice good workstation security measures such as locking up diskettes when not in use, using screen savers with activated passwords appropriately, and positioning screens away from public view.
23. I will immediately notify my manager, Facility Information Security Official (FISO), Director of Information Security Operations (DISO), or Facility or Corporate Client Support Services (CSS) help desk if:
    a. my password has been seen, disclosed, or otherwise compromised
    b. media with Confidential Information stored on it has been lost or stolen;
    c. I suspect a virus infection on any system;
    d. I am aware of any activity that violates this agreement, privacy and security policies; or
    e. I am aware of any other incident that could possibly have any adverse impact on Confidential Information or Company systems.

**Upon Termination**

24. I agree to notify my Physician Support Coordinator within 24 hours, or the next business day, when members of my office staff are terminated, so that user accounts to Company systems are appropriately disabled in accordance with Company standards.
25. 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.
26. Upon termination, I will immediately return any documents or media containing Confidential Information to the Company.
27. I understand that I have no right to any ownership interest in any Confidential Information accessed or created by me during and in the scope of my relationship with the Company.

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

| **Applicant Printed Name** | **Applicant Signature** | **Date** |
|---|---|---|

| **Authorizing Provider Printed Name** | **Authorizing Provider Signature** | **Date** |
|---|---|---|

**PLEASE NOTE:** HCA Medical Staff Office is required to authorize all provider access requests.
**Physicians are required to authorize any office staff requests by signing page 3.**