PHYSICIAN OFFICE STAFF

HCA N. FLORIDA / S. ATLANTIC DIVISION IT&S SECURITY ACCESS REQUEST FORM

ALL FIELDS ON THIS FORM ARE REQUIRED AND MUST BE COMPLETED BEFORE REQUEST WILL BE PROCESSED!
Please be sure to sign the Confidentiality and Security Agreement on page 3 of this document.
QUESTIONS? Call the IT&S Service Desk 888-252-3397

RETURN COMPLETED FORMS TO:

FAX: 1-855-347-9608 or EMAIL: NFDV.PSCAccessRequest@hcahealthcare.com

If submitting forms for multiple users, please send all forms and CSAs together.
Please allow a minimum of two weeks after submission for access to be granted.

ACCESS REQUESTED ☐ **New** ☐ **Modify** ☐ **PSG (HCAPS)** **I need to work/assist onsite in a facility**

Primary Facility: _____ Addt'l Facility: _____

☑ Default Access: Orders, Labs, Imaging Reports, Clinical Notes Comments:

☐ Other (specify): _____

PRACTICE INFORMATION

Practice/Company Name: _____ Specialty: _____

Company address: _____
(STREET CITY STATE ZIP)

Business phone #: _____ Business fax #: _____

Providers at this practice/company/location: _____

Office IT&S contact (full name): _____ Office IT&S contact email: _____

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

Office Manager Signature: _____ Date: _____

PERSONAL INFORMATION

Name: _____
(FIRST MIDDLE LAST)

Home address: _____
(STREET CITY STATE ZIP)

Date of birth: _____ Personal Cell #: _____ *(used for authentication purposes only)*

Email address**:** _____ Role: _____

By signing below, I attest that I have viewed, signed and agreed to the HCA Confidentiality and Security Agreement.

User Signature: _____

PHYSICIAN REQUESTING ACCESS

Credential: _____ Name: _____ NPI: _____
(FIRST MI LASTI)

I will ensure that only appropriate personnel in my office, who have been through a screening process, will access the HCA software systems and confidential information; and I will annually train such personnel on issues related to patient confidentiality and access. I will accept full responsibility for the actions of my employees who may access the HCA software systems and confidential information. I agree that if I, or my staff, stores confidential information on non-HCA media or devices (e.g., PDAs, laptops) or transmits data outside of the HCA 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. 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.

Physician Signature: _____ Date: _____

HCA

Non-Company Employed Practitioner Confidentiality and Security Agreement

I am a practitioner or employed by a practitioner (in the case of office staff) who has clinical privileges and/or membership at an HCA affiliated entity(ies) (the "Company"); or a practitioner or an employee of a practitioner whose patient(s) may have received services from the Company. I desire to access information and/or systems of the Company in order to provide health services to patients. I understand that the Company manages health information and has legal and ethical responsibilities to safeguard the privacy of its patients and their personal and health information ("Patient Information").

Additionally, the Company must protect its interest in, and the confidentiality of, any information it maintains or has access to, including, but not limited to, financial information, marketing information, Company human resources, payroll, business plans, projections, sales figures, pricing information, budgets, credit card or other financial account numbers, customer and supplier identities and characteristics, sponsored research, processes, schematics, formulas, trade secrets, innovations, discoveries, data, dictionaries, models, organizational structure and operations information, strategies, forecasts, analyses, credentialing information, Social Security numbers, passwords, PINs, and encryption keys (collectively, with Patient Information, "Confidential Information").

During the course of my interactions with the Company, I understand that I may access, use, or create Confidential Information. I further acknowledge that I must comply with this Confidentiality and Security Agreement (the "Agreement") and applicable Company policies and procedures at all times as a condition of my accessing Company systems and Confidential Information, and that the Company is relying on such compliance and the representations, terms and conditions stated in this Agreement.

General

1. In connection with accessing Company systems and Confidential Information, I will act in the best interest of the Company and, to the extent subject to it, in accordance with its Code of Conduct at all times.
2. I have no expectation of privacy when using Company systems, including but not limited to Company email accounts (if provided), and/or devices. The Company may log, access, review, store and otherwise utilize information stored on or passing through its systems, devices and network, including email.
3. If I am issued a Company email account, I will only use the account for Company-related business.
4. Any violation of this Agreement may result in the permanent or temporary loss of my access to Confidential Information and/or Company systems, and disciplinary action, including, without limitation, suspension, loss of privileges, loss of medical staff membership, and/or legal action, at Company's sole discretion in accordance with its policies.

Patient Information

5. I will access and use Patient Information only for patients with whom I or my employer has an established treatment relationship and only when it is necessary to provide treatment in accordance with the HIPAA Privacy and Security Rules (45 CFR Parts 160—164), applicable state and/or international laws (e.g., the European Union General Data Protection Regulation), and applicable Company policies and procedures, including, without limitation, its Privacy and Security Policies (available at http://hcahealthcare.com/ethics-compliance/ and the Information Protection Page of the Company's intranet.
6. By accessing or attempting to access a patient's record, I represent to the Company at the time of access that I have the requisite clinical need to know and have the appropriate authorization under applicable law to access the Patient Information.
7. I represent that I or my employer have in effect policies and procedures that comply with applicable law, including without limitation the HIPAA Privacy and Security Rules or the European Union General Data Protection Regulation, as applicable, and shall comply with such policies and applicable laws at all times.

Protecting Confidential Information

8. I acknowledge that the Company is the exclusive owner of all right, title and interest in and to Confidential Information, including any derivatives thereof.
9. I will not publish, disclose or discuss any Confidential Information (a) with others, including coworkers, peers, friends or family, who do not have a need to know it; or (b) by using communication methods I am not specifically authorized to use, including personal email, Internet sites, Internet blogs or social media sites.
10. I will not take any form of media or documentation containing Confidential Information from Company premises unless specifically authorized to do so in order to carry out the purposes for which I have been granted access to Company systems and Confidential Information (collectively, "Authorized Purposes") and in accordance with applicable Company policies.
11. I will not transmit Confidential Information outside the Company network unless I am specifically authorized to do so in order to carry out the Authorized Purposes. If I am authorized to transmit Confidential Information outside of the Company, I will ensure that the information is encrypted according to Company Information Security Standards and ensure that I have complied with applicable Company privacy policies, including the External Data Release policy.
12. I will not retain Confidential Information longer than is necessary to carry out the Authorized Purposes.

Using Mobile Devices, Portable Devices and Removable Media

13. I will not copy, transfer, photograph, or store Confidential Information on any mobile devices, portable devices or removable media, such as laptops, smart phones, tablets, CDs, thumb drives, external hard drives, unless specifically necessary to carry out the Authorized Purposes and these devices or media are secure consistent with applicable law.
14. I understand that any mobile device (smart phone, tablet, or similar device) that synchronizes Company data (e.g., Company email) may contain Confidential Information and as a result, must be protected as required by this Agreement.

Doing My Part – Personal Security

15. I will only access or use systems or devices I am authorized to access, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.

16. I will not attempt to bypass Company security controls.
17. I understand that I will be assigned a unique identifier (i.e., 3-4 User ID) to track my access and use of Company systems and that the identifier is associated with my personal data provided as part of the initial and/or periodic credentialing.
18. In connection with my access to Company systems and Company Information, I will never:
    a. disclose or share user credentials (e.g., password, SecurID card, Tap n Go badge, etc.), PINs, or access codes;
    b. use another individual's, or allow another individual to use my, user credentials (e.g., 3-4 User ID and password, SecurID card, Tap n Go badge, etc.) to access or use a Company system or device;
    c. allow an unauthorized individual to access a secured area (e.g. hold the door open and/or prop the door open);
    d. use tools or techniques to break, circumvent or exploit security measures;
    e. connect unauthorized systems or devices to any Company network; or
    f. use software that has not been licensed and approved by the Company.
19. I will practice good security measures such as locking up media when not in use, using screen savers with passwords, positioning screens away from public view, and physically securing devices.
20. I will immediately notify the appropriate contacts such as the Facility Information Security Official (FISO), Director of Information Security Assurance (DISA), Facility Privacy Official (FPO), Ethics and Compliance Officer (ECO), or Facility or Corporate Client Support Services (CSS) help desk or if involving the United Kingdom, the Data Protection Officer (DPO), Information Governance Manager, Caldicott Guardian, Heads of Governance (HoG), Division Chief Information Security Officer (CISO) if:
    a. My user credentials have been seen, disclosed, lost, stolen, or otherwise compromised;
    b. I suspect media with Confidential Information has been lost or stolen;
    c. I suspect a virus or malware infection on any Company system;
    d. I become aware of any activity that violates this Agreement or any Company privacy or security policies; or
    e. I become aware of any other incident that could possibly have any adverse impact on Confidential Information or Company systems.

Upon Separation

21. I agree that my obligations under this Agreement will continue after termination or expiration of my access to Company systems and Company Information.
22. When my access to Company systems and/or Company Information has been terminated or is no longer needed, for any reason, I will immediately:
    a. securely return to the Company any Confidential Information, Company related documents or records, and Company owned media (e.g., smart phones, tablets, CDs, thumb drives, external hard drives, etc.). I will not keep any copies of Confidential Information in any format, including electronic. However, I am not required to return copies of Patient Information to the extent such information is needed to treat patients as permitted under the HIPAA Privacy and Security Rules; and
    b. un-enroll any non-Company owned devices from the Company Enterprise Mobility Management System, if applicable.

Except to the Extent Otherwise Agreed in a Separate Agreement, the Following Statements Apply

23. I have no intention of varying the volume or value of referrals I make to the Company in exchange for Internet access, access to any Company system or access to any Confidential Information.
24. I have not agreed, in writing or otherwise, to accept Internet access, access to any Company system or access to any Confidential Information in exchange for the referral to the Company of any patients or other business.
25. I understand that the Company may decide at any time, without notice, to no longer provide access to any systems to practitioners on the medical staff or their office 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.
26. I will ensure that only appropriate personnel in my office, who have been through an appropriate screening process, will access the Company systems and Confidential Information. I will annually train such personnel on issues related to patient confidentiality and access.
27. I will accept full responsibility for the actions of my employees who may access the Company software systems and Confidential Information.
28. I agree that if I, or my staff, stores Confidential Information on non-Company media or devices (e.g., mobile devices, laptops) or transmits data outside of the Company network, that the data then becomes my sole responsibility to protect according to applicable law, including the HIPAA Privacy and Security Rules or the European Union General Data Protection Regulation, as applicable, and I will take full accountability for any data loss or breach.
29. I will ensure that members of my office staff use a unique identifier assigned only to them, to access Confidential Information.
30. I agree to notify my Physician Support Coordinator within 24 hours, or the next business day, when members of my office staff are terminated or leave my employment, so that user accounts to Company systems are appropriately disabled in accordance with Company Information Security Standards.
31. To the extent there is a conflict between a term in Sections 23 through 31 and a term separately agreed to in writing with the Company, the term set forth in the separate agreement will control.

By signing this document, I acknowledge that I have read and understand this Agreement, and I agree to be bound by and comply with all the representations, terms and conditions stated herein.

User Signature:	Date:
User Printed Name:	Facility:
Practice:	