Security Access Form (SAF) for 3rd Party Vendors of Hospital-Based Physicians (HBP)

Questions? Contact DivIS.DLEFLPSCs@HCAHealthcare.com or 888-561-3720

STOP! **If the 3rd Party Vendor representative will be onsite at an HCA Healthcare hospital, do not use this form**. The individual must be credentialed as a Verified Professional (VPro)/Dependent Healthcare Professional (DHP) through HealthTrust Workforce Solutions (HWS). HWS will establish the individual's HCA Healthcare 3-4 User ID as part of the credentialing process.

How to Use this Form

1. 3rd Party Vendor representative must provide required* demographic information (noted below) to establish an HCA Healthcare 3-4 ID.
2. Execute the Confidentiality & Security Agreement (CSA) Form - Vendor (also included below).

First Name*	**Middle Initial**	**Last Name***
Home Address*		
City, State, Zip Code*		**Date of Birth***
Personal Phone Number (Mobile)*	**Email Address (assigned by vendor)***	
Employer		

Home address and date of birth purged upon ID creation. Mobile # and email used for password resets.

User access is conditioned upon the obligation of Employer/Provider Group/Physician to notify Company when user's access should be suspended and/or terminated.

Sponsoring Provider Group/Physician*

Provider Group (or Physician Name(s)	
Provider Group/Physician Contact (first and last name)	
Practice Phone Number	**Practice Email Address**

Vendor Confidentiality and Security Agreement

I am an employee, contractor, or agent of a vendor ("Vendor") that provides services to an HCA Healthcare affiliated entity(ies) (the "Company"). I desire to access information and/or systems of the Company in order to provide services to Company on behalf of Vendor (my "Engagement"). 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, Human Resource Information (as defined below), 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 Engagement with the Company, I understand that I may access, use, or create Confidential Information. I agree that I will access and use Confidential Information only when it is necessary to perform the services defined in my Engagement and in accordance with this Confidentiality and Security Agreement (the "Agreement") 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). I further acknowledge that I must comply with this Agreement and such policies and procedures at all times as a condition of my Engagement and in order to access Confidential Information and/or Company systems, and that the Company is relying on such compliance and the representations, terms and conditions stated in this Agreement.

General

1. In connection with my Engagement with the Company, I will act in the best interest of the Company and, to the extent subject to it, in accordance with its Code of Conduct.
2. I have no expectation of privacy when using Company systems and/or devices. The Company may log, access, review, and otherwise utilize information stored on or passing through its systems, devices and network, including email.
3. Any violation of this Agreement may result in the loss of my access to Confidential Information and/or Company Systems, disciplinary and/or legal action, including, without limitation, suspension, and/or termination of my Engagement with the Company, at Company's sole discretion in accordance with its policies.

Patient Information

4. I will access and use Patient Information only as necessary to perform my assigned job duties in accordance with the HIPAA Privacy and Security Rules (45 CFR Parts 160—164) and, as applicable, with state laws and international regulations (e.g., the European Union General Data Protection Regulation).
5. I will request and access the minimum amount of Patient Information required to carry out my job duties related to my Engagement.
6. By accessing or attempting to access Patient Information, I represent to the Company at the time of access that I have the requisite job duty and Engagement-related need to know and have the appropriate authorization under applicable law to access the Patient Information.

Protecting Confidential Information

7. I acknowledge that the Company is the exclusive owner of all right, title and interest in and to Confidential Information, including any derivatives thereof.
8. 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.

9. I will not take any form of media or documentation containing Confidential Information from Company premises unless specifically authorized to do so as part of my Engagement and in accordance with applicable Company policies.
10. I will not transmit Confidential Information outside the Company network unless I am specifically authorized to do so as part of my Engagement. 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.
11. I will not retain Confidential Information longer than required to carry out the Engagement, and in no event longer than required by Company's Record Retention Policy.
12. I will only reuse or destroy media in connection with the Engagement in accordance with the Company's Information Security Standards.
13. I acknowledge that in the course of the Engagement, I may have access to human resource information, which may include compensation, age, sex, race, religion, national origin, disability status, medical information, criminal history, personal identification numbers, addresses, telephone numbers, financial and education information (collectively, "Human Resource Information"). I understand that I am allowed to discuss any Human Resource Information about myself and other individuals if they self-disclose their information. I can also discuss Human Resource Information that does not relate to my individual Engagement and that is not in violation of any other provision in this Agreement.

Using Mobile Devices, Portable Devices and Removable Media

14. 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 required and authorized to do so as part of my Engagement with the Company.
15. 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

16. 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.
17. I will not attempt to bypass Company security controls.
18. 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 and/or employment verification.
19. In connection with the Engagement, I will never:
    a. disclose or share user credentials (e.g., password, SecurID card, Tap n Go badge, etc.), PINs, access codes, badges, or door lock 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 computer system or device;
    c. allow a non-authorized individual to access a secured area (e.g. hold the door open, share badge or door lock code, 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 the Company network; or
    f. use software that has not been licensed and approved by the Company.
20. I will practice good workstation 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 workstations while traveling or accessing Company systems remotely.
21. I will immediately notify my sponsor, 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 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

22. I agree that my obligations under this Agreement will continue after termination or expiration of my access to Company systems and/or Company Information.
23. At the end of my Engagement with the Company 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; and
    b. un-enroll any non-Company owned devices from the Company Enterprise Mobility Management System, if applicable.

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.

Signature	Date
Printed Name	3-4 User ID
Vendor Name	