Verified Professional Member Confidentiality and Security Agreement

I understand that the HCA affiliated entity(ies) (the "Company") for which I am a Verified Professional Member (my "Engagement") manages health information and has legal and ethical responsibilities to safeguard the privacy of its patients and their personal and health information ("Patient Information"). "Verified Professional Member" means employees, employed Licensed Independent Practitioners (LIPs) (*e.g.,* employed/managed physicians), employed Advanced Practice Professionals (APPs), residents/fellows, students (*e.g.*, nursing, medical, and interns), faculty/instructors, contractors (*e.g.*, HealthTrust Verified Professional Solutions (HWS), travelers, network/per diem staff, or dependent healthcare professionals and/or contracted through another temporary staffing agency), and volunteers.

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 patients' information, "Confidential Information"). The Company must also protect Company Property (such as inventions, software, trade secrets, and Developments (as defined below)).

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 my job-related duties and in accordance with the Company's 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 such policies, procedures, and this Confidentiality and Security Agreement (the "Agreement") at all times as a condition of my Engagement and in order to obtain authorization for access to Confidential Information and/or Company systems. I acknowledge that the Company is relying on such compliance and the representations, terms and conditions stated herein.

General

1. 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 during my Engagement with the Company.
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, or other disciplinary and/or legal action, including, without limitation, suspension, loss of privileges, 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 for patients whose information I need to perform my assigned job duties in accordance with the HIPAA Privacy and Security Rules (45 CFR Parts 160—164), applicable state and 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).
5. I will only access, request and disclose the minimum amount of Patient Information needed to carry out my assigned job duties or as needed for treatment purposes.
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-related need to know and 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 IInformation, 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 job and in accordance with 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 job responsibilities. 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 the External Data Release policy and other applicable Company privacy policies.
11. I will not retain Confidential Information longer than required by the Company's Record Retention policy.
12. I will only reuse or destroy media in accordance with the Company's Information Security Standards.
13. I acknowledge that in the course of performing my job responsibilities 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 employees if they self-disclose their information. I can also discuss Human Resource Information that does not relate to my individual employment or my job responsibilities 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 Company Information Security Standards.

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 my 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 codes, 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 and working remotely.
21. I will immediately notify my manager, 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 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.

Except to the Extent Otherwise Agreed in a Separate Agreement, the Following Statements Apply to All Verified Professional Members

24. I shall promptly disclose to the Company all Company Property that I develop during my Engagement. "Company Property" means any subject matter (including inventions, improvements, designs, original works of authorship, formulas, processes, compositions of matter, software, databases, confidential information and trade secrets), whether belonging to the Company or others, that, directly or indirectly: (i) I author, make, conceive, first reduce to practice, or otherwise create or develop, whether alone or with others using any Company equipment, supplies, facilities, or Confidential Information, or (ii) otherwise arises from work performed by me for the Company, its employees, or agents, (each of the foregoing, a "Development").
25. As between me and the Company, all Company Property is the property of the Company or its designee, and all copyrightable Developments that I create within the scope of my employment are "works made for hire."
26. I agree to assign, and do hereby irrevocably assign, to the Company or its designee all of my right, title, and interest in and to any and all Developments, together with all intellectual property and other proprietary rights therein or arising therefrom, including any registrations or applications to register such rights and the right to sue for past, present, or future infringements or misappropriations thereof.
27. During and after my Engagement, I agree to execute any document and perform any act to effectuate, perfect, enforce, and defend the Company's rights in any Development. I hereby appoint the Company and its authorized agent(s) as my attorney in fact to execute such documents in my name for these purposes, which power of attorney shall be coupled with an interest and shall be irrevocable, if I fail to execute any such document within five (5) business days.
28. If there is a conflict between a term in Sections 24 through 28 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.

Signature	Date
Printed Name	