SCOPE: All Company-affiliated facilities including, but not limited to, hospitals, ambulatory surgery centers, physician practices, home health agencies, service centers, and all Corporate Departments, Groups and Divisions.

PURPOSE: To promote awareness about individual and external entity responsibility for protecting Company information and to authorize and require agreements with individuals and external entities to acknowledge accountability for protecting Company information including confidential patient information, Social Security numbers, financial account information, personnel information, provider credentialing information, or other sensitive information regardless of format (e.g., electronic, paper, oral).

POLICY:

A. **Information Confidentiality and Security Agreement (CSA) with Individuals.** The CSA form acknowledges specific responsibilities the individual has in relation to information security and the protection of sensitive information from unauthorized disclosure or use. These individual obligations support federal regulations for confidentiality and security, including the HIPAA Privacy and Security Rules and the European Union’s General Data Protection Regulation. The following individuals must sign and abide by the applicable CSA form:

1. All Company workforce members including 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 Workforce Solutions (HWS) travelers, network/per diem staff, or dependent healthcare professionals and/or contracted through another temporary staffing agency), and volunteers who are granted access to Company information, or granted access to Company-provided systems must sign and abide by the Workforce Member CSA.

2. All non-Company employed LIP and their non-Company employed office or support staff (i.e., those providing a service to a physician), who are granted access to Company information systems, or granted access to the Internet through Company provided systems, or granted access to Confidential patient information must sign and abide by the Non-Company Employed Practitioner CSA.

3. Representatives of vendors working on Company premises and/or granted access to Company information systems (onsite or remotely) or Company sensitive information must sign the Vendor CSA form. A non-Company-employed individual or other external entity shall enforce such CSAs on behalf of the vendor’s employees or contractors working off-site (e.g., contracted transcription service, electronic claims submissions.
support contractor, physician office practice (i.e., those providing a service to the Company), if stipulated in the Company’s contract with the external entity (see B. below).

4. Representatives of an insurer or other third party payer working on Company premises and/or granted access to Company information systems (onsite or remotely) or Company sensitive information must sign the Payer CSA form.

All individuals subject to a CSA form may be required by HCA Information Protection and Security to re-sign the CSA form annually or when HCA Information Protection and Security makes significant revisions to the CSA form and those revisions are approved by the Ethics & Compliance Policy Committee. Privileged providers will re-sign the CSA form at each reappointment. An individual working at or providing services for multiple HCA facilities is required to sign only one CSA form, but is still subject to re-signing requirements.

The CSA forms are official Company documents and must not be altered in any manner without prior approval from HCA Information Protection and Security.

**B. Contracts with Business Partners.** Relationships with an external entity involving access to Company information and Company information systems or the exchange, transmission, or use of sensitive Company information require a formal contract including provisions to protect the confidentiality and security of the information and/or information systems. For more information, refer to the Information Security - Vendor Information Security Agreement Policy, IP.SEC.008.

**C. Contracts for External IT&S Services.** All contracts for external services will include appropriate standard security language approved by IT&S and Legal. Refer to Information Security - Vendor Information Security Agreement Policy, IP.SEC.008.

**D. Sanctions.** Violations of this policy could lead to disciplinary measures up to and including termination of employment or business relationship. Suspected violations of this policy are to be handled in accordance with the Discipline section of the Code of Conduct. The Company encourages resolution at the local level and each Customer (an organization, business entity or organizational unit that has an established business relationship with an external IT&S organization as described in this policy’s scope) will designate a process for reporting violations. In addition, violations may be reported to the Ethics Line at 1-800-455-1996.

**E. Policy Exceptions.** Exceptions to Policy are to be submitted to HCA Information Protection and Security for review and approval.
**PROCEDURE:**

A. The CSA form templates are maintained by HCA Information Protection and Security and posted on the Company Intranet.

B. Before an employee, resident/fellow, student (e.g., nursing, medical or intern), faculty/instructor, contractor (e.g., HWS traveler, network/per diem staff, dependent healthcare professional and/or independent contractors and employees of non-HWS staffing agencies), or volunteer is granted any access to Company information or Company information systems (except for access to an electronic CSA course), the individual must sign a CSA form (e.g., electronic signature).

1. Human Resources must ensure the CSA form is signed and maintained in the employee’s personnel file (e.g., digitally stored) in accordance with record series code HUM-70-04 *Human Resources - Personnel Files Active Employee Personnel Files*.

2. HWS must ensure the CSA form is signed and maintained in the Company’s records about the traveler, network/per diem staff, or dependent healthcare professional (e.g., digitally stored) in accordance with HUM-70-02 *Human Resources – Personnel Files Temporary Employee Personnel Files*.

3. The sponsor of independent contractors (or contractors of non-HWS staffing agencies) and students (e.g., nursing, medical, or intern) must ensure the CSA form is signed and maintained in the Company’s records about the individual (e.g., digitally stored) in accordance with HUM-70-02 *Human Resources – Personnel Files Temporary Employee Personnel Files*.

C. Each LIP and APP (privileged practitioners) must sign the appropriate CSA form at the time he or she is initially appointed to a facility’s medical staff as part of the credentialing process.

1. Completed CSA form will be maintained in the individual’s credentials file (e.g., digitally stored in Cactus) as described in the Licensure and Certification Policy, CSG.QS.002.

2. Retention of the CSA form varies according to state law in accordance with record series code XX-MED-10-07 *Administrative Offices, Medical Staff Files*.

D. Each LIP and APP (non-privileged practitioners) must sign the appropriate CSA form after completion of favorable license and eligibility checks by Medical Staff Services (MSS), but prior to granting any access to Company information or Company information systems.

1. Completed CSA forms will be maintained by MSS in the individual’s credentials file (e.g., digitally stored) as described in the Licensure and Certification Policy, CSG.QS.002.
2. Retention of the CSA form varies according to state law in accordance with record series code XX-MED-10-07 Administrative Offices, Medical Staff Files.

E. Physician office and support staff must sign Non-Company Employed Practitioner CSA form at the time information access is granted.
   1. Completed CSA forms will be maintained (e.g., digitally stored) in a central location.
   2. Retention of the CSA form varies according to state law in accordance with record series code XX-MED-10-07 Administrative Offices, Medical Staff Files.

F. Each volunteer must sign the Workforce Member CSA form before beginning his or her service. The CSA form signature process can be completed during Code of Conduct training (if the volunteer attends such training), volunteer orientation, or separately.

   The sponsor of the volunteer must ensure the CSA form is signed and maintained in the Company’s records of the volunteer’s service (e.g., digitally stored) in accordance with record series code XX-MED-10-16 Administrative Offices, Volunteer Records.

G. Representatives of vendors and other external entities must sign the Vendor CSA form, or equivalent confidentiality agreement, when vendor representatives are assigned to work onsite with access to Company information, or if the individual vendor representative is granted access to Company systems (either onsite or remotely). The vendor representative must sign the Vendor CSA form before information access or system access is granted.

   Completed Vendor CSAs must be maintained in the individual contract folder (e.g., in Novatus) by the Facility CFO or designee in accordance with record series code LEG-20-01 Legal - Contracts/Agreements Contracts/Agreements – General.

H. Representatives of insurers or other third party payers must sign the Payer CSA form, or equivalent confidentiality agreement, when representatives are assigned to work onsite with access to Company information, or if the individual representative is granted access to Company systems (either onsite or remotely). The representative must sign the Payer CSA form before information access or system access is granted.

   Completed Payer CSAs must be maintained in the individual contract folder (e.g., in Novatus) by the Facility CFO or designee in accordance with record series code LEG-20-01 Legal - Contracts/Agreements Contracts/Agreements – General.
<table>
<thead>
<tr>
<th>DEPARTMENT: Information Protection and Security</th>
<th>POLICY DESCRIPTION: Information Confidentiality and Security Agreements</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAGE: 5 of 5</td>
<td>REPLACES POLICY DATED: 8/15/01, 11/1/01, 1/27/04, 4/30/05, 3/1/07, 12/1/07, 10/1/10, 9/1/11, 12/1/13, 4/1/16</td>
</tr>
<tr>
<td>EFFECTIVE DATE: January 1, 2018</td>
<td>REFERENCE NUMBER: IP.SEC.005 (formerly IS.SEC.005)</td>
</tr>
<tr>
<td>APPROVED BY: Ethics and Compliance Policy Committee</td>
<td></td>
</tr>
</tbody>
</table>

**REFERENCES:**

1. [Code of Conduct Site](#)
2. Information Security – Program Requirements Policy, [IP.SEC.001](#)
4. Information Security ISA site on Atlas
5. [IP Standard: Mobile Device Management AC.MCT.02](#)
6. [IP Standard: Mobile Device Encryption AC.MCT.03](#)
7. [IP Standard: Mobile Device Applications AC.MCT.04](#)
8. Electronic Communications Policy, [IP.SEC.002](#)
9. Physician Access to the Internet Policy, [LL.026](#)
10. Copyright Policy, [LL.GEN.002](#)
11. Records Management Policy, [EC.014](#)
12. [EC.014 Records Management Policy Attachment D: Record Retention and State Specific Record Retention Schedules](#)
13. Appropriate Use of Company Communications Resources and Systems Policy, [EC.026](#)
14. [Background Investigations, HR.ER.002 (Model Policy)](#)
15. [Licensure and Certification, CSG.QS.002](#)
16. [Vetting Dependent Healthcare Professionals and Other Non-Employees, CSG.QS.003](#)
17. “Encryption” Atlas Connect site
18. “Identifying Sensitive Data” Atlas Connect site
[This page intentionally left blank.]
Workforce Member Confidentiality and Security Agreement

I understand that the HCA affiliated entity(ies) (the “Company”) for which I am a Workforce 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”). “Workforce 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 Workforce 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 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 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 Workforce 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.

<table>
<thead>
<tr>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Printed Name</td>
<td>3/4 ID</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Printed Name</th>
<th>3/4 ID</th>
</tr>
</thead>
</table>
[This page intentionally left blank.]
Vendor Confidentiality and Security Agreement

I am an employee, contractor, or agent of a vendor ("Vendor") that provides services to an HCA 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.

<table>
<thead>
<tr>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Printed Name</td>
<td>3/4 ID</td>
</tr>
</tbody>
</table>
[This page intentionally left blank.]
Payer Confidentiality and Security Agreement

I am an employee, contractor, or agent of an insurer or other third party payer ("Payer") whose enrollees or beneficiaries have received, or are receiving, services from the Company ("Enrollees). I desire to access information and/or systems of the Company in order to provide services to Enrollees on behalf of Payer (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, 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 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 for patients who are Enrollees of Payer and only to perform my health care operations services on behalf of Payer in accordance with the HIPAA Privacy and Security Rules (45 CFR Parts 160—164) and Payer’s policies.
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.

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.

10. I will only reuse or destroy media in connection with the Engagement in accordance with the Company’s Information Security Standards.

applicable Company privacy policies, including the External Data Release policy.

11. I will only reuse or destroy media in connection with the Engagement in accordance with the Company’s Information Security Standards.

Using Mobile Devices, Portable Devices and Removable Media

12. 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.

13. 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

14. 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.

15. I will not attempt to bypass Company security controls.

16. 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.

17. In connection with the Engagement, I will never:

   a. disclose or share user credentials (e.g., 3-4 User ID and 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.

18. 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.

19. 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 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

20. I agree that my obligations under this Agreement will continue after termination or expiration of my access to Company systems and Company Information.

21. At the end of my Engagement with the Company for any reason, I will immediately 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 except to the extent such information is needed by Payer to provide services to Enrollees as permitted under the HIPAA Privacy and Security Rules.

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.

<table>
<thead>
<tr>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Printed Name</td>
<td>3/4 ID</td>
</tr>
</tbody>
</table>