DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Information Confidentiality and Security Agreements
PAGE: 1 of 5	**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, 1/1/18
EFFECTIVE DATE: August 1, 2020	**REFERENCE NUMBER:** IP.SEC.005 (formerly IS.SEC.005)
APPROVED BY: Ethics and Compliance Policy Committee	

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).

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Information Confidentiality and Security Agreements
PAGE: 2 of 5	**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, 1/1/18
EFFECTIVE DATE: August 1, 2020	**REFERENCE NUMBER:** IP.SEC.005 (formerly IS.SEC.005)
APPROVED BY: Ethics and Compliance Policy Committee	

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 Healthcare Information Protection & Security to re-sign the CSA form annually or when HCA Healthcare Information Protection & 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 Healthcare 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 Healthcare Information Protection & 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 ITG Services.** All contracts for external services will include appropriate standard security language approved by ITG 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 ITG 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 or http://hcahealthcareethicsline.ethix360.com.

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

PROCEDURE:

A. The CSA form templates are maintained by HCA Healthcare Information Protection & 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-70-04 Human Resources - Personnel Files Active 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-70-04 Human Resources - Personnel Files Active 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, COG.PPA.002.
   2. The CSA form is retained in accordance with record series code HUM-70-04 Human Resources - Personnel Files Active Employee Personnel 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, COG.PPA.002.
   2. The CSA form is retained in accordance with record series code HUM-70-04 Human Resources - Personnel Files Active Employee Personnel 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. The CSA form is retained in accordance with record series code HUM-70-04 Human Resources - Personnel Files Active Employee Personnel Files.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Information Confidentiality and Security Agreements
PAGE: 4 of 5	**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, 1/1/18
EFFECTIVE DATE: August 1, 2020	**REFERENCE NUMBER:** IP.SEC.005 (formerly IS.SEC.005)
APPROVED BY: Ethics and Compliance Policy Committee	

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 HUM-70-04 *Human Resources - Personnel Files Active Employee Personnel Files.*

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 HUM-70-04 *Human Resources - Personnel Files Active Employee Personnel Files.*

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 HUM-70-04 *Human Resources - Personnel Files Active Employee Personnel Files.*

REFERENCES:

1. Code of Conduct Site
2. Information Security – Program Requirements Policy, IP.SEC.001
3. Information Security – Vendor Information Security Agreement (ISA) Policy, IP.SEC.008
4. Information Security ISA site on Atlas
5. IP Standard: Enterprise Mobility Management OIS.MDT.02
6. IP Standard: Mobile Device Encryption OIS.MDT.03
7. IP Standard: Mobile Device Management OIS.MDT.04
8. Electronic Communications Policy, IP.SEC.002
9. Physician Access to the Internet Policy, LL.026
10. Copyright Policy, LL.GEN.002

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Information Confidentiality and Security Agreements
PAGE: 5 of 5	**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, 1/1/18
EFFECTIVE DATE: August 1, 2020	**REFERENCE NUMBER:** IP.SEC.005 (formerly IS.SEC.005)
APPROVED BY: Ethics and Compliance Policy Committee	

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, COG.PPA.002
16. Vetting Dependent Healthcare Professionals and Other Non-Employees, COG.PPA.003
17. “Encryption” Atlas Connect site
18. “Identifying Sensitive Data” Atlas Connect site
19. Non-Company Employed Practitioner CSA Form
    a. English
    b. Spanish
20. Payer CSA Form
    a. English
    b. Spanish
21. Vendor CSA Form
    a. English
    b. Spanish
22. Workforce Member CSA Form
    a. English
    b. Spanish