DEPARTMENT: Ethics and Compliance	**POLICY DESCRIPTION**: Appropriate Use of Electronic Communication Resources and Systems
PAGE: 1 of 8	**REPLACES POLICY DATED:** 7/1/09, 9/15/10, 11/15/10, 4/1/11, 8/15/13, 6/1/14, 5/1/15, 11/1/16, 2/1/19, 9/1/19, 1/1/22
EFFECTIVE DATE: November 1, 2024	**REFERENCE NUMBER:** EC.026
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: This Policy applies to all HCA Healthcare affiliated facilities worldwide including, but not limited to, hospitals, ambulatory surgery centers, home health agencies, hospice agencies, physician practices, outpatient imaging centers, service centers, Parallon, HealthTrust, Sarah Cannon Cancer Network and all Corporate Departments, Groups, Divisions and Markets (individually and collectively the "Company").

PURPOSE: This Policy sets the parameters for the following uses of Company owned or provided Information Technology Systems, Electronic Communication passing through such systems and Digital Media and the Company's access to such usage to monitor, review and retrieve any usage activity or content pursuant to this Policy and other Company policies:

1. Intracompany use of Company owned or provided Information Technology Systems, Electronic Communication and Digital Media;
2. Use of Company owned or provided Information Technology Systems, Electronic Communication and Digital Media to access or transmit information to or from personal or other third-party Information Technology Systems, Electronic Communication or Digital Media;
3. Use of third-party (including public, private and personal) Information Technology Systems, Electronic Communication and Digital Media when the User holds themselves out as being employed by or representing the Company, can be perceived as speaking on behalf of the Company or uses or discloses the Company's confidential or proprietary business information; and
4. Use of or access to AI Solutions when one of the other three conditions are met.

POLICY: Anyone who accesses, uses or transmits data through Company owned or provided Information Technology Systems, Electronic Communication, Digital Media or AI Solutions are subject to this Policy, including but not limited to employees or authorized non-employees. For purposes of this Policy, all persons identified as being within the scope of this Policy are referred to as "User" singularly or "Users" collectively.

A. **Business Purpose and Use.** The Company encourages the use of Electronic Communication and Digital Media to promote efficient and effective communication in the course of conducting Company business. Electronic Communication and information made available through Company owned or provided Information Technology Systems are Company property, and their primary purpose is to facilitate Company business. Users must not use unapproved external, third-party e-mail or information technology systems to conduct Company business. Users have the responsibility to use Electronic Communication in a professional, ethical, and lawful manner in accordance with the Company's Code of Conduct and policies.

B. **Personal Communications.** When a User communicates in their personal capacity (i.e., not on behalf of the Company), it is important that the User not create the impression that they are communicating on behalf of the Company. User must comply with all appropriate safeguards

of Company confidential and proprietary information as articulated in the Company Code of Conduct and policies.

C. **No Expectation of Privacy.** A User shall presume no expectation of privacy in anything they may access, use, create, store, send or receive on or through Company owned or provided Information Technology Systems, Electronic Communication and Digital Media. The Company reserves the right to monitor, access, review and retrieve any activity or content on or transmitting through Company owned or provided Information Technology Systems, Electronic Communication and Digital Media without the User's consent.

D. **Electronic Communication Content.** Content of all Electronic Communication should be truthful and accurate, sent to recipients on a need-to-know basis and sent or posted with appropriate privacy and security measures applied in accordance with the Information Security Standards and Privacy policies, which are available on the Company's intranet site under Information Protection & Security Department.

E. **Use of Digital Media.** The use of Digital Media is governed by detailed guidelines located on the Company's intranet site. The guidelines address Company-authorized use of Digital Media and personal use of Digital Media. A User is responsible for reviewing and adhering to the HCA Healthcare Digital Media Guidelines. Nothing in the HCA Healthcare Digital Media Guidelines can be used to limit, constrain, or waive rights guaranteed employees by federal law (e.g., Section 7 of the National Labor Relations Act) or rights granted pursuant to a Collective Bargaining Agreement. Any submission of information through generative Artificial Intelligence tools or platforms must be in accordance with the Company's Responsible AI Policy (EC.031).

F. **Use of Personally-Owned Mobile Devices to Access Information on Company Information Technology Systems.** Workforce members, other than those exempted in Mobile Device Security Standards, must enroll their personally-owned mobile devices in the Company's mobile device management program before accessing Company owned or provided Information Technology Systems from their mobile devices, unless otherwise allowed by the Company.

G. **Exceptions.** Although rare, exceptions to this Policy may be granted by the Senior Vice President and Chief Ethics and Compliance Officer. Requests for such exceptions should be submitted in writing to the Chief Security Officer and Vice President and Senior Vice President and Chief Ethics and Compliance Officer or the Vice President Ethics and Compliance responsible for administration of the Ethics Line.

PROCEDURE:

A. **Productive and Appropriate Communication.** Every User has a responsibility to protect the Company's public image and to use Company owned or provided Information Technology Systems, Electronic Communication and Digital Media in a productive and appropriate manner. Users must avoid communicating anything that might appear unprofessional or inappropriate or might be misconstrued as inappropriate by a reader. Communications which should be avoided by Users include but are not limited to communications that are obscene, malicious, threatening, harassing, or that discriminate or could contribute to a hostile work

environment on the basis of race, color, religion, gender, national origin, age, disability, sexual orientation, gender identity, genetic information, protected veteran status, or any other status protected by law or Company policy.

B. **Personal Communications Using Company Communication Systems.**

The Company recognizes that Users may occasionally need to conduct personal business during their work hours and permits highly limited, reasonable personal use of the Company's Information Technology Systems and Electronic Communication for such purpose.

Any personal use of the Company's Information Technology Systems and Electronic Communication is subject to all the provisions of this Policy and related Company policies. Any questions related to a User's personal use of the Company's Information Technology Systems and Electronic Communication are to be directed to the User's manager.

C. **Personal Communications.**

When a User is communicating personally, as opposed to on behalf of the Company, the User must make it clear that their communication is on their own behalf and does not represent the views of the Company. When using any form of Digital Media, the User must comply with the HCA Healthcare Digital Media Guidelines located on the Company's intranet site and all other applicable policies.

D. **Monitoring and Accessing Information and Electronic Communication.**

1. The Company may monitor, log, review, retrieve and otherwise utilize information stored on or transmitting through Company owned or provided Information Technology Systems in order to assess the appropriateness of the communications or content, manage its Information Technology Systems and enforce Company policies. The Company may also capture User activity within its Information Technology Systems, including but not limited to Internet history and communications to and from third parties.
2. The Company reserves the right to use content management tools to monitor comments, posts or discussions about the Company, its employees, its patients and the industry posted on the Internet.
3. The Company reserves the right, at any time and without prior notice, to monitor, log, review, retrieve and otherwise utilize Electronic Communication, files, documents, personal file directories, Electronic Media, or any other information stored or accessed via Company Information Technology Systems.
    a. This monitory activity is performed to assure compliance with Company policy, support the performance of internal investigations, and assist with the management of Company's Information Technology Systems.
    b. Information contained in Electronic Communications, including but not limited to documents, attachments, embedded links, and any other information concerning the use of Company's Information Technology Systems may be disclosed to the appropriate authorities, both inside and outside of the Company, to document misconduct or criminal activity. Moreover, in some situations, the Company may be

required to disclose Electronic Communication even if such communications or information are marked private or intended only for limited internal distribution.

4. The Company may block the transmission of information across Information Technology Systems, or a User's access and/or usage of Information Technology Systems, for the purpose of protecting Company resources.
5. Any evidence of violation of Company policy discovered during monitoring must be reported to the User's manager.

E. **Request for Access to Electronic Communications.**

1. Except as otherwise stated in this Policy, any request for access, review or retrieval of a User's Electronic Communications, personal files or Internet history logs must be approved by the Senior Vice President and Chief Ethics and Compliance Officer, in accordance with this Policy. Prior to access, review or retrieval of a User's Electronic Communications, personal files or Internet history logs, a request must be submitted to the responsible corporate Ethics Line Case Manager on the Electronic Communications Monitoring Request (ECMR) form by one of the following individuals:
   a. Ethics & Compliance Officer (ECO)
   b. Human Resources
   c. Business Protection Executive (BPE)
   d. Director of Information Security Assurance (DISA)
   e. Facility Information Security Official (FISO) or Zone FISO
   f. Any member of senior leadership at the Facility, Market, Division, Group
2. Corporate Department requests to access, review or retrieve a User's Electronic Communications, personal files or Internet history logs must be submitted to the responsible Ethics Line Case Manager by the respective Corporate Department's Vice President.
3. The Ethics Line Case Manager will consult with Corporate Employment Counsel regarding such request prior to seeking Senior Vice President and Chief Ethics and Compliance Officer approval of the ECMR.
4. Under the following limited circumstances, the ECO, BPE, DISA, Zone FISO or a Corporate Department Vice President, as applicable, may approve a request to access,

review or retrieve a User's Electronic Communications, personal files and Internet history logs without submission or approval of an ECMR:

a. To dispose of or reassign a User's personal files after a User has left the Company;

b. To access critical files when a User is absent and access to those files is necessary for operational continuity;

c. To research or respond to Company Information Technology System performance or security issues;

d. Upon request of the Legal Department, to respond to an administrative demand, subpoena or in connection with any other legal proceedings; or

e. To conduct an audit of a User's activity within Company Information Technology Systems without accessing or reviewing any content (e.g., number/size of messages sent and received, access to EHR/medical records, Information Technology Systems login/logout data).

5. Notwithstanding anything to the contrary in this Policy, a User's Electronic Communications, personal files or Internet history logs may be accessed, reviewed and retrieved in support of an information security investigation upon approval of the Chief Security Officer and Vice President, without an ECMR or the foregoing approval procedures.

F. **Internet Use.** Users may only access or download information or content from appropriate Internet sites in accordance with Company Information Security Standards and the Code of Conduct.

G. **Artificial Intelligence Use**. Users may only access or use Artificial Intelligence tools or platforms in accordance with the Company's Responsible AI Policy (EC.031).

H. **Considerations related to Use of Company Email and Webex Accounts.**

1. Heightened cybersecurity concerns are associated with a non-employee's use of a Company email account that could lead to the introduction of malware into the Company's network (i.e., clicking a link or opening an attachment). Associated risks can be mitigated by adding non-employed practitioners to the "external email opt out" group.

2. Non-employees given Company email accounts appear to be "employees" in the Outlook Global Address List (GAL) and in Webex (i.e., no warning banner that non-employees are included in a Webex chat or internal email string).

3. Non-employees given Company email accounts may be privy to internal communications and/or sensitive information not intended for disclosure to external parties.

4. Non-employees using Company email accounts may appear to represent HCA Healthcare when communicating with external parties.

5. Physician or other non-employed provider communications for the delivery of direct patient care should occur only through approved clinical communication tools. Company email and Webex are not intended to be used in place of clinical communication tools.
6. Before assigning a Company email account and/or Webex to a physician or other authorized non-employee, such individual must first sign the HCA Healthcare Confidentiality and Security Agreement (CSA), acknowledging that: (i) HCA Healthcare may store and access the emails or Webex spaces at any time, and (ii) the email or Webex account should be used only for HCA Healthcare related business.
7. Any physician or other authorized non-employee assigned a Company email account and/or Webex must be notified during onboarding processes about appropriate use of internal communication tools.
8. If a physician group/practice is no longer contracted to provide services to any HCA Healthcare affiliated facilities, the practice's domain (e.g., @TexasOrtho.com) must be removed timely from the list of approved ("green listed") external domains and the Company email and/or Webex account for each physician associated with the practice must be terminated timely.
9. Physicians and other authorized non-employees may not be approved for "expanded" internet access (EIA) to access personal/external email accounts (i.e., must use personal device/phone).

I. **Unacceptable Uses of Company Information Technology Systems, Electronic Communication and Digital Media.** Users may not use Company owned or provided Information Technology Systems, Electronic Communication, Digital Media or other means of communication in any of the following ways:

1. To harass, intimidate, make defamatory statements, or threaten another person or organization.
2. To access or distribute obscene, sexually explicit, abusive, libelous, or defamatory material.
3. To illegally obtain or distribute copyrighted material that is not authorized for reproduction/ distribution.
4. To impersonate another User or third party or mislead a recipient about one's identity..
5. To access another person's e-mail, if not specifically authorized to do so.
6. To bypass Company Information Technology Systems security mechanisms.
7. To transmit unsecured Highly Sensitive or Sensitive Company information.
8. To initiate or forward chain letters or chain e-mail.
9. To send unsolicited mass e-mail ("spamming") to persons with whom the User does not have a prior relationship.
10. To participate in political or religious debate.

11. To automatically forward messages (e.g., with mailbox rules) to Internet e-mail addresses.
12. To communicate the Company's official position on any matter, unless specifically authorized to make such statements on behalf of the Company.
13. To pursue a business interest that is unrelated to the Company.
14. To engage in any conduct that violates the Company's policy on solicitation or distribution.
15. To deliberately perform acts that waste computer resources or unfairly monopolizes resources.
16. For any other purpose which is illegal or against Company policy.

J. **Reporting and Handling Violations.** Each facility must designate a process for promptly reporting violations of this Policy. Typically, such process would include reporting to one's supervisor, another member of management, a Human Resources representative, the ECO, the FPO or the DISA, FISO or Zone FISO. In addition, suspected violations may be reported to the Ethics Line at 1-800-455-1996 or http://hcahealthcareethicsline.webline.sai360.net

K. Investigation and resolution at the local level is encouraged. Suspected violations of this Policy must be handled in accordance with this Policy, the Code of Conduct, HCA Healthcare Digital Media Guidelines and other relevant Company policies.

DEFINITION:

AI Solution: refers to Artificial Intelligence and Machine Learning technologies both individually and collectively, unless otherwise specified within the context of its use. Refer to the Responsible AI Policy (EC.031) for further information concerning Artificial Intelligence and Machine Learning.

Digital Media: refers to any and all digital technology, platform and/or practice (both now existing or existing in the future) that enables people to use, create, share, or otherwise interact or engage with content, individuals, communities, opinions, insights, and/or conversations over the internet. Digital Media may include external Company owned or authorized Digital Media (e.g., Facebook, Instagram, LinkedIn, YouTube, X) internal Company-owned Digital Media (Intranet, internal blogs and message boards) and a User's personal Digital Media posts, accounts (e.g., Facebook, Instagram, TikTok, YouTube, X), and any content created, posted or shared within such technology or platform.

Electronic Media: refers to any device that may be used to store or transport data (e.g., internal and external hard drives, CDs, DVDs, and USB drives).

Electronic Communication: refers to a means of communication that allows individuals to use computerized systems or devices for communication, including but not limited to e-mail, Internet services, team rooms (e.g., Webex Teams), Instant Messages, virtual meeting platforms (e.g., WebEx, Zoom, Microsoft Teams), chat services, file share drives, databases, blogs, microblogs, applications and any form of Digital Media, including any content transmitted, captured or stored within such systems or devices.

Information Technology Systems: refers to, but is not limited to: computer workstations, networks, servers, databases, network drives, clinical systems (e.g., Meditech, iMobile,

DEPARTMENT: Ethics and Compliance	**POLICY DESCRIPTION**: Appropriate Use of Electronic Communication Resources and Systems
PAGE: 8 of 8	**REPLACES POLICY DATED:** 7/1/09, 9/15/10, 11/15/10, 4/1/11, 8/15/13, 6/1/14, 5/1/15, 11/1/16, 2/1/19, 9/1/19, 1/1/22
EFFECTIVE DATE: November 1, 2024	**REFERENCE NUMBER:** EC.026
APPROVED BY: Ethics and Compliance Policy Committee	

PatientKeeper), file share platforms (e.g., SharePoint), data storage devices, file transfer utilities, software applications, AI Solutions, Company-provided devices (including Company-provided mobile devices), personal mobile devices that are authorized via Mobile Device Management (MDM) to connect to the Company network, any associated infrastructure for such systems and any Electronic Communication or Digital Media content transmitted, captured or stored within such systems.

User: refers to employees and authorized non-employees including but not limited to contractors, physicians, advanced practice professionals, students, volunteers, vendor representatives or any other individual providing services to or on behalf of HCA Healthcare who accesses, uses or transmits information to or from Company Information Technology Systems and Electronic Communication resources.

REFERENCES:

1. Code of Conduct
2. Employee Handbook
3. Equal Employment Opportunity, Anti-Harassment and Respectful Workplace Policy, HR.ER.072
4. Solicitation Policy, HR.OP.030
5. Information Confidentiality and Security Agreements Policy, IP.SEC.005
6. Information Security – Electronic Communications Policy, IP.SEC.002
7. IS Standard: Enterprise Mobility Management, OIS.MDT.02
8. IS Standard: Mobile Device Encryption, OIS.MDT.03
9. IS Standard: Mobile Device Management, OIS.MDT.04
10. HIPAA Privacy Policies
11. HCA Healthcare Digital Media Guidelines
12. Electronic Communications Monitoring Request form
13. Responsible AI Policy, EC.031