DEPARTMENT: Ethics and Compliance	**POLICY DESCRIPTION:** Appropriate Use of Communications Resources and Systems
PAGE: 1 of 6	**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
EFFECTIVE DATE: September 1, 2019	**REFERENCE NUMBER:** EC.026
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: This Policy applies to all Company-affiliated facilities including, but not limited to, hospitals, ambulatory surgery centers, home health centers, hospice centers, physician practices, outpatient imaging centers, service centers and all Corporate Departments, Groups, Divisions and Markets.

This Policy applies to anyone who uses Company electronic communication and information systems ("IT systems"), including, but not limited to:

- Employees;
- Contractors;
- Physicians;
- Volunteers; and
- Representatives of vendors and business partners.

Unless otherwise indicated, this Policy applies to the use of any Company IT systems, including, but not limited to:

- workstations and terminal devices
- networks, servers, and associated infrastructure;
- software and applications, including clinical systems and communication systems such as e-mail, instant messaging, file transfer utilities, and blogs; and
- databases, files shares, team rooms (*e.g.* Webex Teams), and data storage devices.

This Policy applies to the use of Company IT systems to access *non-company* systems on the Internet or at external companies including, but not limited to:

- connection to external non-Company networks and devices;
- connection to Internet sites and external Web-based applications;
- use of external e-mail (*e.g.*, Gmail), instant messaging, blogs, micro-blogs (*e.g.*, Twitter), chat services, and other social media communications and applications; and
- use of external data storage and file sharing sites and applications.

This Policy also applies to the use of systems, applications, Internet sites or other electronic media other than Company IT systems (*e.g.*, personal or public computers) by employees, contractors, physicians, volunteers and representatives of vendors and business partners when they:

1. hold themselves out as being employed by or representing the Company or an affiliated facility;
2. can be perceived to be speaking on behalf of the Company or an affiliated facility; or
3. use confidential or otherwise protected information obtained through their employment or affiliation with the Company or an affiliated facility.

DEPARTMENT: Ethics and Compliance	**POLICY DESCRIPTION:** Appropriate Use of Communications Resources and Systems
PAGE: 2 of 6	**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
EFFECTIVE DATE: September 1, 2019	**REFERENCE NUMBER:** EC.026
APPROVED BY: Ethics and Compliance Policy Committee	

For purposes of this Policy, all persons identified as being within the Scope of this Policy (*i.e.,* employees, contractors, physicians, volunteers and representatives of vendors and business partners) are referred to as "User" singularly or "Users" collectively.

PURPOSE: This Policy sets the parameters for use of communication resources, particularly electronic resources, such as e-mail, Internet services and social media.

POLICY:

1. **Business Purpose and Use.** The Company encourages the use of electronic communication resources, including but not limited to: email, Internet services, team rooms, chat services, file shares, databases, blogs, microblogs, applications, instant messaging, social media and other electronic means ("Electronic Communications") to promote efficient and effective communication in the course of conducting Company business. Electronic Communications and information made available through Company IT systems are Company property, and their primary purpose is to facilitate Company business. Employees must not use external e-mail or systems to conduct Company business. Users have the responsibility to use Electronic Communications in a professional, ethical, and lawful manner in accordance with the Company's Code of Conduct.

2. **Personal Communications.** When a User communicates in his/her personal capacity (*i.e.*, not on behalf of the Company), it is important that the User not create the impression that he/she is communicating on behalf of the Company. The User must comply with all appropriate safeguards of Company information as articulated in the Company Code of Conduct and policies.

3. **No Expectation of Privacy.** A user shall presume no expectation of privacy in anything he or she may access, create, store, send or receive on or through Company IT systems. The Company reserves the right to monitor and/or access communications usage and content without the User's consent.

4. **Communications Content.** Content of all communications should be truthful and accurate, sent to recipients based on a need-to-know and sent or posted with appropriate security measures applied in accordance with the Information Security Standards, which are available on Atlas Connect under Information Protection & Security Department.

5. **Use of Social Media.** The use of social media (as defined below) is governed by detailed guidelines located on the Company's intranet. The guidelines address Company-authorized use of social media and personal use of social media. Each User is responsible for reviewing and adhering to the Company's Social Media Guidelines.

Nothing in the social media guidelines can be used to limit, constrain, or waive rights guaranteed employees by federal labor law (*e.g.*, Section 7 of the National Labor Relations Act) or rights granted pursuant to a collective bargaining agreement.

6. **Use of Personally-Owned Mobile Devices to Access Information on Company IT 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 information from their mobile devices.

7. **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 Vice President & Chief Information Security Officer or the Vice President, Ethics and Compliance, responsible for administration of the Ethics Line.

DEFINITION:

Social Media are online communication methods in which individuals play an active role as both the author and audience of messages and comments, including but not limited to, blogs, bulletin boards, networks (*e.g.*, Facebook, Twitter), multi-media (*e.g.*, YouTube, Instagram) and news media sites.

PROCEDURE:

1. **Productive and Appropriate Communication.** Every User has a responsibility to protect the Company's public image and to use communication resources and Company IT systems in a productive and appropriate manner. Users must avoid communicating anything that might appear inappropriate or might be misconstrued as inappropriate by a reader, for example 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.

2. **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 IT systems for such purpose.

   Any personal use of the Company's IT systems is subject to all the provisions of this and related Company policies. Any questions are to be directed to the appropriate managers.

3. **Personal Communications.**
When a User is communicating personally, as opposed to on behalf of the Company, the User must make it clear that his/her communication is on his/her own behalf and does not represent the views of the Company. When using social media, the User must comply with the Social Media Guidelines located on the Company's intranet.

4. **Monitoring.**
   a. The Company may log, review, and otherwise utilize information stored on or passing through its IT systems in order to review communications, manage its IT systems and enforce Company Policy. The Company may also capture User activity within its IT systems, including but not limited to Internet sites visited and access to non-Company systems.

   b. 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 by anyone.

   c. The Company reserves the right, at any time and without prior notice, to examine files, documents, personal file directories, hard disk drive files, Electronic Communications or any other information stored on Company IT systems.
      1. This examination is performed to assure compliance with Company Policy, support the performance of internal investigations, and assist with the management of Company IT systems.
      2. Information contained in documents or Electronic Communications and any other information concerning the use of Company IT may be disclosed to the appropriate authorities, both inside and outside of the Company, to document employee misconduct or criminal activity. Moreover, in some situations, the Company may be required to publicly disclose communications or information, including e-mail messages, even if such communications or information are marked private or intended only for limited internal distribution.

   d. Any evidence of violations of Company policy discovered during monitoring must be reported to the appropriate managers.

5. **Access to Communications Resources and Electronic Communications**.
   a. Any review or retrieval of a User's Electronic Communications 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 review or retrieval of a User's Electronic Communications 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 the Facility Ethics & Compliance Officer (ECO), Human Resources representative, Director of Information Security Assurance (DISA), Facility Information Security Official (FISO)

or Zone FISO, or a member of senior leadership at the Facility, Division or Market. Corporate Department requests to review or retrieve Electronic Communications or Internet history logs must be submitted to the responsible Ethics Line Case Manager by the respective Corporate Department's Vice President. The Ethics Line Case Manager will consult with Corporate Employment Counsel regarding the request for review or retrieval of a User's Electronic Communications and Internet history logs prior to submitting the ECMR to the Senior Vice President and Chief Ethics and Compliance Officer for review and approval.

b. A Users' personal files, including those on Company IT systems and computers, must generally be handled with the same privacy given to personal mail and personal phone calls. This means that other workers, including managers and information systems administrators, must not read a User's personal files without approval of an ECMR, as described above.

c. Under the following limited circumstances, the Facility ECO, DISA, FISO, Zone FISO or a Corporate Department Vice President, as applicable, may approve a request to access or retrieve a User's Electronic Communications and Internet history logs without submission of an ECMR:
   1. To dispose of or reassign a User's personal files after a User has left the Company.
   2. To access critical files when a User is absent and access to those files is necessary for operational continuity.
   3. To research or respond to Company IT system performance or security issues.
   4. Upon request of the Legal Department, to respond to an administrative demand, subpoena or in connection with other legal proceedings; or
   5. To conduct an audit of a User's activity within Company IT systems without accessing or reviewing any content (*e.g.,* number/size of messages sent and received, access to EHR/medical records, IT systems login/logout data).

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

7. **Unacceptable Uses.** Users may NEVER use the Company's IT systems, Internet access, e-mail, or other means of communication in any of the following ways:
   a. To harass, intimidate, make defamatory statements, or threaten another person or organization.
   b. To access or distribute obscene, sexually explicit, abusive, libelous, or defamatory material.
   c. To illegally obtain or distribute copyrighted material that is not authorized for reproduction/ distribution.
   d. To impersonate another user or mislead a recipient about one's identity.

e. To access another person's e-mail, if not specifically authorized to do so.
f. To bypass Company IT systems security mechanisms.
g. To transmit unsecured confidential information.
h. To initiate or forward chain letters or chain e-mail.
i. To send unsolicited mass e-mail ("spamming") to persons with whom the User does not have a prior relationship.
j. To participate in political or religious debate.
k. To automatically forward messages (*e.g.,* with mailbox rules) to Internet e-mail addresses.
l. To communicate the Company's official position on any matter, unless specifically authorized to make such statements on behalf of the Company.
m. To pursue a business interest that is unrelated to the Company.
n. To engage in any conduct that violates the Company's Policy on solicitation or distribution.
o. To deliberately perform acts that waste computer resources or unfairly monopolizes resources.
p. For any other purpose which is illegal or against Company Policy.

8. **Sanctions.** Suspected violations of this Policy must be handled in accordance with this Policy, the Code of Conduct, any Company sanctions and enforcement policies and the Company's Social Media Guidelines. Investigation and resolution at the local level is encouraged and each Facility must designate a process for promptly reporting violations. Typically, this includes reporting to one's supervisor, another member of management, a Human Resources representative, the Facility ECO, or the DISA, FISO or Zone FISO. In addition, suspected violations may be reported to the Ethics Line at 1-800-455-1996.

REFERENCES:

1. Code of Conduct
2. Employee Handbook
3. Equal Employment Opportunity Policy, HR.ER.013
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: Mobile Device Management AC.MCT.02
8. IS Standard: Mobile Device Encryption AC.MCT.03
9. IS Standard: Mobile Device Applications AC.MCT.04
10. HIPAA Privacy Policies
11. HCA Healthcare Social Media Guidelines
12. Electronic Communications Monitoring Request form