DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Information Security - Electronic Communications
PAGE: 1 of 4	**REPLACES POLICY DATED:** 1/1/99, 8/15/01, 11/30/04, 4/30/05, 1/1/09, 7/1/09
EFFECTIVE DATE: January 1, 2018	**REFERENCE NUMBER:** IP.SEC.002 (formerly IS.SEC.002)
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: This policy applies to all Users of 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, and data storage devices.

This policy also 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 Web 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 Networking communications applications; and
- use of external data storage and file sharing sites and applications.

PURPOSE: This policy is designed to protect the Company, its personnel, its patients, its data, and its resources from the risks associated with use of Company IT systems.

POLICY: Company Information Security standards apply to any use of Company IT systems, including use of Company IT systems to connect to or access non-company systems such as Internet sites and applications.

Example: Users must comply with Company information security policies and standards any time they utilize a Company workstation, whether for Company business or to connect to the Internet for personal reasons.

PROCEDURE:

1. **Use of Company IT systems.**
   a. Company IT systems are Company property and are intended for legitimate business use.

b. External, non-Company systems are not to be used in place of company IT systems to conduct Company business.
   Example: Users are not to use external email (*e.g.,* Gmail or Hotmail) in place of Company email (Outlook or MOX) when conducting Company business.

c. Users are permitted reasonable use of Company-IT systems for personal use, as long as the use is in accordance with Company Information Security standards, policy set forth in the Appropriate Use of Company Communication Resources and Systems Policy, EC.026, and the Company Code of Conduct.

d. Users are permitted to utilize Company IT systems to access certain approved external (Internet) sites for reasonable personal use as long as that use is in accordance with Company Information Security standards, EC.026, and the Company Code of Conduct.

e. The Company reserves the right to block access to any external non-Company site.

f. Users must not use non-Company systems to bypass security controls on Company IT systems.

g. Users must not establish connections with non-company networks without the approval of IT&S Network Services. Please refer to Information Security Guidance: External Connectivity.

2. **Monitoring.**
   a. The Company reserves the right to monitor any User activity on Company IT systems, including email and access to non-Company systems.

   b. Users' IT system activity (*e.g.*, number and size of messages sent and received, Internet sites visited, length of time spent using the Internet) on Company IT systems is monitored, *e.g.*, email messages may be monitored and screened.

   c. Any evidence of violations of Company policy discovered during monitoring must be reported to the appropriate managers for follow-up action, in accordance with E&C Policy EC.026.

3. **Confidential Information Transmittal.**
   a. Confidential information, as defined in the Information Security Standards and the Company's Code of Conduct, that requires transmission to external non-Company systems may only be transmitted via Company IT systems (*e.g.*, email or file transfer systems)

b. Appropriate agreements must be in place between the involved parties, such as a Business Associate Agreement, an Information Security Agreement, or an Information Confidentiality and Security Agreement. (*See* Information Confidentiality and Security Agreements Policy, IP.SEC.005.)

c. Confidential information which is transmitted via IT systems to external non-Company systems must be encrypted. For directions on how to encrypt email and files in accordance with Information Security Standards, please refer to the "Sending Sensitive Information" page on the Information Protection Atlas site.

d. Confidential information must not be posted on publicly accessible areas of the Internet (*e.g.*, discussion groups, bulletin boards, chat services, non-secured web sites).

4. **Malicious Code Protection.** Each User must take reasonable precautions to avoid introducing viruses and other malicious code into the Company's networks.
   a. Users on Company IT systems must not download programs from external Internet sites unless approved by Users' supervisors and needed to perform Users' job functions.
      Example: Users should not download screen savers, tools, or games from Internet sites to Company workstations without approval.

   b. Unexpected e-mail attachments and attachments in e-mails from unknown parties must not be opened without first validating the source.

   c. All Users must have the Company's standard anti-virus utility properly installed and running on their PCs, and keep pattern files used to recognize malicious computer programs updated in accordance with Information Security Standards.

5. **Remote Access Authentication.** Users will be "strongly" authenticated into the Company's network when accessing the network. Strong authentication requires the use of a network user-ID and password from Company facilities, and a second authentication factor such as a token or certificate for remote access. Due to the nature of changing technologies, the method to strongly authenticate an individual, process or program will be defined in the Information Security Standards.

6. **Policy Exceptions.** The Company's Chief Information Security Officer establishes information security governance processes. Requests for exceptions should be sent to Information Protection and Security via e-mail. Exception approval is based upon risk management reflecting appropriate, reasonable, and effective information security measures for a given situation.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Information Security - Electronic Communications
PAGE: 4 of 4	**REPLACES POLICY DATED:** 1/1/99, 8/15/01, 11/30/04, 4/30/05, 1/1/09, 7/1/09
EFFECTIVE DATE: January 1, 2018	**REFERENCE NUMBER:** IP.SEC.002 (formerly IS.SEC.002)
APPROVED BY: Ethics and Compliance Policy Committee	

REFERENCES:

1. Code of Conduct
2. Appropriate Use of Company Communication Resources and Systems Policy, EC.026
3. Health Insurance Portability and Accountability Act, Security Standards for the Protection of Electronic Protected Health Information, 45 CFR Parts 160, 162, and 164
4. Information Security – Program Requirements, IP.SEC.001
5. Information Confidentiality and Security Agreements Policy, IP.SEC.005
6. Information Protection - Release of Company Data to External Entities, IP.GEN.004
7. Information Security Standards
8. Information Security Guidance: External Connectivity
9. Patient Privacy Policies, IP.PRI.001 through IP.PRI.010
10. Sending Sensitive Information (Information Protection Atlas page)
11. Copyright Policy, LL.GEN.002
12. Records Management Policy, EC.014
13. Electronic Communication Privacy Act