POLICY & PROCEDURE	Page 1 of 4
SUBJECT: Email and Communication Systems IS-054	EFFECTIVE Date: 10/01/2010
DEPT: INFORMATION SYSTEMS	REVIEW Date: 02/04/2016

Purpose:

The purpose of this policy is to outline the requirements for E-mail and *communication system*[*] usage at Inspira Health Network. Inspira Health Network's electronic mail and other communication systems, such as voice mail, are designed to facilitate business communications and are not to be used in a way that may be disruptive, offensive to others or harmful to morale. The requirements outlined in this policy serve to protect *Inspira Health Network workforce*[*], customers, members and *external entities*[*] and to secure *corporate information assets*[*]. Local, state, and federal laws affect this policy.

Scope:

This policy and all related procedures define the minimum requirements for Inspira Health Network e-mail and communication system usage and need to be met by all members of the Inspira Health Network workforce. Please refer to the Acceptable Use Supplement to IS 054 for detailed guidance on email and communication systems.

Policy:

A. Requirements

A.1 E-mail

a) General Use

E-mail is a substitute for a written memo and should be treated as such by members of the Inspira Health Network workforce. Inspira Health Network E-mail systems shall be used primarily for business use. Personal use of Inspira Health Network E-mail systems shall be limited to a level that does not impede worker productivity. The content of all E-mails shall be used in a way that does not disrupt or offend others, harm morale or create security exposures. Members of the Inspira Health Network workforce shall ensure that the business information contained in E-mail messages is accurate, appropriate and lawful. When sending email attachment files, caution shall be taken by members of Inspira Health Network's workforce that the correct file is being attached. User authentication shall be performed (by the sender) during the transmission of all Inspira Health Network Emails to ensure that the content is only accessible by the intended recipient.

b) Emailing Sensitive Corporate Information Assets

It is strongly recommended that confidential corporate information assets be omitted from all E-mails and E-mail attachments sent or forwarded outside Inspira Health Network's network by members of the Inspira Health Network workforce. All sensitive Inspira Health Network corporate information assets (including financial and proprietary information) transmitted outside Inspira Health Network's network via Email shall be encrypted during transmission according to formally documented procedures that outline current acceptable Inspira Health Network encryption standards. All external Email transmissions containing sensitive Inspira Health Network corporate information assets shall remain encrypted until the information reaches its final destination.

A.2 Communication Systems

a) General Use

Information generated and/or transmitted via Inspira Health Network communication systems, in addition to the communication systems themselves, is considered to be a valuable and sensitive Inspira Health Network corporate information asset. Inspira Health Network communication systems shall be used primarily for business use. Personal use of Inspira Health Network communication systems shall be limited to a level that does not impede worker productivity. Members of the Inspira Health Network workforce shall ensure that business information contained in messages communicated via Inspira Health Network communication systems is accurate, appropriate, and lawful.

b) Transmitting Sensitive Corporate Information Assets

Confidential information can be relayed via communication systems only after the requirements for entity authentication (see IS-060 Password Control for requirements) and appropriate clearances and authorization (see IS-061 Personnel Security for requirements) are fulfilled.

A.3 E-mail and Communication System Privacy

It is the Policy of Inspira Health Network and its affiliated organizations that all emails that are sent by any Inspira Health Network employee through the use of a computer that is owned or provided by Inspira Health Network, including laptops, or other company owned or issued equipment may not be considered confidential by the employee. This includes emails that are sent via an employee's personal, web-based, password-protected e-mail account, such as, but not limited to, Yahoo Mail or G-Mail.

Messages generated within and/or transmitted through Inspira Health Network E-mail and/or communication systems are neither private nor confidential to the employee. Inspira Health Network

reserves the right to intercept, monitor, access, and/or disclose any information that is maintained on, stored in or transmitted through its E-mail or communication systems for any purpose.

Upon *separation of service**, members of the Inspira Health Network workforce shall not retain any rights to contents of the Inspira Health Network E-mail and/or communications systems.

All messages distributed via Inspira Health Network E-mail and all other communication systems provided by Inspira Health Network are subject to monitoring by the Information Security Team, and disclosure to law enforcement or government officials or to other third parties through subpoena or other lawful processes.

A.6 Disclaimer

E-mail and communication system messages generated by members of the Inspira Health Network workforce may not necessarily reflect the views of Inspira Health Network, its officers, directors or management.

B. Responsibilities

B.1 Inspira Health Network Management

Inspira Health Network management shall ensure their staff adheres to the requirements outlined in this policy and all subordinate procedures related to E-mail and communication systems. Management staff must also follow all requirements in this policy and related procedures and immediately report any known breach of corporate security policy to Corporate Compliance or to the Information Security Team.

B.2 Inspira Health Network Workforce

All members of the Inspira Health Network workforce shall comply with this policy and all referenced policies to ensure privacy of sensitive corporate information assets. Members of the Inspira Health Network workforce shall report any known breach of this policy and/or its subordinate procedures to a member of their management or the Information Security Team or Corporate Compliance. Members of the Inspira Health Network workforce will be aware of compliance with the E-mail Acceptable Use Policy.

B.4 Corporate Information Systems Security Personnel

The Information Security Team shall maintain and update all policies related to E-mail and communication system usage to ensure that they are comprehensive and consistent with local, state, and federal law. Information Security shall ensure that all responsibilities for carrying out the requirements outlined within this policy are delegated to qualified staff. Information Security reserves the right to intercept, monitor, access, and/or disclose any information that is maintained on, stored in or transmitted through its E-mail or communication systems for any purpose. Information Security shall be made aware of any breach of corporate security policy and advise Human Resources and Corporate Compliance as to the severity of the breach.

C. Accountability

Employees and users of Inspira Health Network corporate information assets who are found to be in violation of any part of this policy are subject to disciplinary action, up to and including termination of employment or contract and legal action. Retaliatory action shall not be taken against individuals who identify and/or report violations of security policy.

* Term is defined in Appendix A-Glossary of Terms.