<table>
<thead>
<tr>
<th><strong>Subject</strong></th>
<th>Security and Electronic Messaging Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attachments</strong></td>
<td>□ Yes  ☒ No</td>
</tr>
<tr>
<td><strong>Key words</strong></td>
<td>Messaging, email, e-mail, instant messaging, IM</td>
</tr>
<tr>
<td><strong>Category</strong></td>
<td>Management of Information (MI)</td>
</tr>
<tr>
<td><strong>Number</strong></td>
<td>GHI-SEC-100-2</td>
</tr>
<tr>
<td><strong>Effective Date</strong></td>
<td>29-September-2008</td>
</tr>
<tr>
<td><strong>Manual</strong></td>
<td>Information Security Policy</td>
</tr>
<tr>
<td><strong>Last Review Date</strong></td>
<td>16-April-2011</td>
</tr>
<tr>
<td><strong>Issued By</strong></td>
<td>IS&amp;T Security Management</td>
</tr>
<tr>
<td><strong>Next Review Date</strong></td>
<td>16-April-2012</td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td>This policy applies to Group Health Plan, Inc. and all of its operating units and related organizations (collectively, “HealthPartners/ GHI”).</td>
</tr>
<tr>
<td><strong>Implementation Date</strong></td>
<td>29-September-2008</td>
</tr>
<tr>
<td><strong>Retired Date</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Roles and Responsibilities**
Owner: IS&T Security Management
Reviewer: IS&T Sr. Vice President and CIO

**Standards are currently under development**
I. **PURPOSE**

This policy defines the protection for all electronic messaging. This includes and is not limited to:

- Electronic mail (e-mail)
- Instant messaging (IM)
- Text messages
- Messages sent via Pagers

This policy covers appropriate use of any electronic messages sent from a corporate e-mail address and/or corporate network, systems, applications, workstations and mobile devices, and in addition, applies to all employees, consultants, vendors, and agents operating on behalf of HealthPartners, Inc / GHI.

II. **POLICY**

**Access**

- Delegated access may be granted to another user in the e-mail system and must be approved by the owner of the user account that will be accessed.
- Employees, consultants and agents of HealthPartners / GHI are responsible for all messages sent or forwarded from their e-mail account.
- All users are responsible for closing out and logging off of their e-mail account when not in use, specifically on shared computers to prevent unauthorized use and access of e-mail accounts.

**Privacy and Security**

The security and privacy of messages cannot be guaranteed. During the course of system maintenance, IS&T staff may inadvertently view the contents of messages as they are processed through the e-mail system. Staff members are expected to maintain the confidentiality of the data and may be subject to disciplinary action up to, and including termination.

- Employees should not consider e-mail to be private, secure or guaranteed.
- E-mail is not private like a telephone.
- E-mails addressed to non-existent or incorrect recipients may be delivered to unintended recipients.

Any transmission of Protected Information through e-mail must follow the Organizational Privacy Standards for Using E-mail to Communicate With and About Patients and Members and Sending Protected Information Securely.

**Monitoring**

The e-mail system has been installed to facilitate the business of HealthPartners / GHI. All e-mail messages and logs are company records. HealthPartners / GHI reserves and will exercise the right to review, monitor, audit, intercept, access or disclose, as appropriate, the contents of any and all e-mail communications. HealthPartners / GHI will monitor messages without prior notice and are obligated to monitor all electronic messages. No advance notice or approval is required.
Employees, consultants, or agents of HealthPartners / GHI should NOT expect privacy of any access or communication conducted over e-mail.

Prohibited Activities

The HealthPartners / GHI e-mail system shall not be used for the creation or distribution of any disruptive, threatening or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, national origin, or violates state or federal law in any way.

Employees, consultants or agents of HealthPartners / GHI who receive any e-mails with this content from any HealthPartners / GHI employee, consultant or agent are expect to report the matter to their supervisor immediately.

E-mail and other electronic messages transmitted information must not:

- Contain copyrighted material unless the permission of the copyright owner has been obtained, or it is done under fair use guidelines.
- Violate HealthPartners / GHI sexual harassment policy.
- Be used for commercial use outside of HealthPartners / GHI.
- Appear to represent itself as official HealthPartners / GHI communication without appropriate permission.
- Appear to misrepresent the identity of the sender.
- Contain material which violates pornography laws.
- Contain mobile code that could cause a security breach or permit use of resources in opposition to HealthPartners / GHI policy.

Personal Use

Employees, consultants, or agents of HealthPartners / GHI should limit their use of these systems for business and clinical purposes, except for incidental and occasional personal use that does not:

- Interfere with normal business activities.
- Adversely impact employees’ job performance.
- Involve pursuing and/or promoting any outside business activity not associated with HealthPartners / GHI.
- Embarrass or potentially embarrass HealthPartners / GHI.
- Otherwise violate this or other policies.

Users should use the same care in drafting e-mail and other electronic messages as they would for any other communication. Users are expected to craft e-mail messages in a professional manner; rule of thumb is to write in the style of a letter or memo. Since most e-mail is text based, it is difficult to communicate humor, warmth, sensitivity and other emotions. Be careful, since these emotions can be taken out of context.

** Standards are currently under development **
**Instant Messaging**

Only approved Instant Messaging (IM) software will be installed or used (Communicator); unapproved external 3rd party vendors is prohibited.

**Mail Retention and Backup**

In order to accommodate e-mail system growth:

- User quotas will be set on a per user basis. Users will get a message that they are out of space, but will still be allowed to receive new e-mails. If the user quota is over the limit, the sending of e-mail will be temporarily blocked until the message store size is reduced and is under the quota. It is the user’s responsibility to delete or archive messages, or request an increase in his or her quota. Quota increases may be denied. Please reference the associated Electronic Messaging Standards** for current standards on quota limits.

- There is a limited period of time that e-mail messages, appointments, tasks or notes will be able to be restored. Please reference the associated Electronic Messaging Standards** for current standards on retention periods.

**Internet E-mail**

Internet addresses will be in the form of firstname.mi.lastname@healthpartners.com, but other domain names are possible (i.e. westfieldshospital.com). An incremental number will be appended onto the end of the name if a duplicate name exists.

- The security and delivery of messages sent outside of HealthPartners / GHI cannot be guaranteed.
- E-mail messages are limited to a set maximum size which also includes attachments. Please reference the associated electronic messaging standards** for current message size limitations.
- Due to issues with SPAM, viruses and other forms of malware, certain attachments are blocked. Please see the associated standards** on current extensions that are blocked.
- Delete e-mails without opening from unknown and unexpected senders, especially e-mails with attachments. Suspicious e-mails can be reported to spamreview@healthpartners.com.

All e-mail sent externally from HealthPartners / GHI will include the following footer:

“This e-mail and any files transmitted with it are confidential and are intended solely for the use of the individual or entity to which they are addressed. If you are not the intended recipient or the individual responsible for delivering the e-mail to the intended recipient, please be advised that you have received this e-mail in error and that any use, dissemination, forwarding, printing, or copying of this e-mail is strictly prohibited.

If you have received this e-mail in error, please immediately notify the IS&T Support Center by telephone at 952-967-6600. You will be reimbursed for reasonable costs incurred in notifying us.”

**Standards are currently under development**
Email Address Forwarding and Blocking

- E-mail accounts will be expired on the last day of employment. Requests can be made to the immediate supervisor to forward any personal mail within 10 days of final day of employment.
- Automatic forwarding to an external email account is prohibited and blocked.
- SMTP email relaying is prohibited and blocked. Only approved SMTP email relays will be allowed.

E-mail Access and Mobile Device Support

- External e-mail access is allowed through Outlook Web Access (OWA) or Citrix applications. Two-factor authentication is required for remote e-mail access.
- POP3 and IMAP protocols are prohibited and are blocked by HealthPartners / GHI e-mail servers.
- Mobile devices with remote access let employees synchronize with the HealthPartners / GHI e-mail system.
- Corporate e-mail can only be synched to a HealthPartners approved phone and only with approved Wireless E-mail Access software from the Desktop Standards list (GoodLink or ActiveSync). It is prohibited to synch a HealthPartners approved phone to another phone or to synch to your personal accounts (i.e. personal folders, email, contacts, & calendars) and/or to use unapproved Wireless E-mail Access software for data synchronization to the HealthPartners network (MobileMe). Please note, it is acceptable to view your personal e-mail from your phone, but prohibited to synch your HealthPartners e-mail to your personal e-mail account via your phone.
- E-mail account delegation is required by the synchronization service to synchronize e-mail with the mobile device, through approved the standards, GHI-SEC-200-6-1, Cell Phone/PDA Standard. Accounts with domain admin privileges are prohibited from using e-mail through mobile devices.

HIPAA Compliance

- Any e-mail containing Protected Information must follow the Using E-mail to Communicate With and About Patients and Members and the Sending Protected Information Securely Organizational Privacy Standards.
- Due diligence is required when sending an e-mail with Protected Information to ensure that the email recipient corresponds to the intended recipient. Any e-mail containing Protected Information that is misdirected MUST BE reported to the Office of Integrity and Compliance at privacy@healthpartners.com or 952-883-5124.
- Do not send Protected Information via e-mail using personal or web e-mail programs (for example, Gmail, Hotmail, Yahoo or Comcast accounts).
- Do not send Protected Information via e-mail to your personal e-mail account(s).
- Use only a secure transmission method when sending Protected Information outside of the organization via e-mail: Secure Mail tool, E-transfer, TLS, or encrypted process performed by IS&T’s EDI team.
- E-mail messages containing Protected Information will not be forwarded to non-HealthPartners / GHI e-mail addresses.

**Standards are currently under development**
PCI DSS Compliance

In adherence with our mission to ensure the security and privacy of our members, patients, customers, colleagues and in the interests of our organizations, credit card numbers are not to be sent via e-mail, it is a security risk.

1. Sending member and patient credit card numbers is prohibited and may result in disciplinary action, up to and including discharge.
2. It is against the HealthPartners, Inc. /Regions Hospital Purchasing Travel Card (PCARD) Program’s policy and procedures to send your card holder account number via e-mail.
3. In efforts to prevent identity theft, we strongly encourage you to not send your personal credit card numbers via e-mail.

III. PROCEDURE(S)
N/A

IV. RISK
Adherence to HealthPartners policies and procedures reduces the risk of exposure of HealthPartners / GHI information assets.

V. DEFINITIONS
E-mail - The electronic transmission of information through an electronic mail protocol such as SMTP or IMAP. HealthPartners / GHI has standardized on Microsoft Outlook e-mail client.
Encryption – a tool used to make information unreadable unless someone has a password.
Forwarded e-mail – E-mail resent from an internal network to an outside point.
Chain e-mail - Email that is sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
POP3 – Email protocol used to retrieve email from a system.
IMAP – Email protocol used to retrieve email from a system.
SMTP – Email protocol used to send email to a system.
PHI – Patient Health Information.
HIPAA – Healthcare Information Portability and Accounting Act.
IM – Instant Messaging. A real-time text messaging protocol.

VI. COMPLIANCE
Failure to comply with this policy or the associated standards and procedures may result in disciplinary action, up to and including termination.

VII. MONITORING AND MEASUREMENT
This policy will be reviewed annually to determine its timeliness and relevance.

VIII. ATTACHMENTS
N/A

** Standards are currently under development **
IX.  OTHER RESOURCES
ISO 27002:2005 Section 10.8
HealthPartners Sexual Harassment Policy – C303
E-Mail Use – Attorney-Client Privileged Information – C407
E-Mail Use – Credentialing and Peer Review Activities – C408
E-Mail Use – Employment Information – C409
E-Mail Use – Trade Secrets and Other Confidential Business Information – C410
E-Mail Etiquette
Code of Conduct - C401/CI001
Using E-mail to Communicate With and About Patients and Members, Organizational Privacy Standard
Sending Protected Information Securely, Organizational Privacy Standard
HealthPartners / GHI-SEC-200-6-1, Cell Phone/PDA Standards

** Standards are currently under development **