I. PURPOSE
This policy defines the protection for all electronic messaging. This includes and is not limited to:
- Electronic mail (email)
- Instant messaging (IM)
- Text messages
- Messages sent via Pagers
- Voicemail

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

II. POLICY
Access
- Delegated access may be granted to another user in the email 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 email account.
- All users are responsible for closing out and logging off their email account when not in use, specifically on shared computers to prevent unauthorized use and access of email 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 email 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 email private, secure or guaranteed.
- Emails addressed to non-existent or incorrect recipients may be delivered to unintended recipients.

Any transmission of Protected Information through email 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 electronic messaging systems have(s) been installed to facilitate the business of HealthPartners/GHI. All electronic 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 electronic message 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 email.*

**Prohibited Activities**
The HealthPartners/GHI electronic messaging systems 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 emails with this content from any HealthPartners/GHI employee, consultant or agent are expected to report the matter to their supervisor immediately.

Emails and other electronic messages transmitting 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.
- 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.

**USE OF DISTRIBUTION LISTS**
The e-mail system is a Company resource dedicated to meeting the needs of the organization and a distribution list created by the Employer may not be used for an employee’s personal use except for
a distribution list created by the Employer for the employee’s own area/department/clinic (provided that such personal use of a distribution list does not otherwise constitute a Prohibited Use or include Prohibited Content in violation of HR policy C406. If an employee creates his/her own distribution list to be used for the employee’s personal use, it should be of a limited size.

**Personal Use**
Incidental and occasional personal use of the employer’s electronic communication tool is permitted provided it does not:

- Interfere with normal business activities.
- Adversely impact employees’ job performance.
- Involve performing outside employment, operating or promoting the employee’s own business, or pursuing similar personal commercial ventures.
- Otherwise violate this policy or other policies of the Employer, including the Employer’s Human Resources policies regarding e-mail and Internet usage.

**Instant Messaging (IM)**
Only approved instant messaging software will be installed or used (Microsoft Lync). Other instant messaging systems, such as provided by 3rd party vendors, are not approved and should not be used: they are prohibited.

**Mail Retention and Backup**
In order to accommodate email system growth:

- There is a limited period of time that email messages, appointments, tasks or notes will be able to be restored. Please reference the HealthPartners/GHI Record Retention Policy for current standards on retention periods.

**Internet Email**
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.
- Email messages are limited to a set maximum size, which also includes attachments.
- Due to issues with SPAM, viruses and other forms of malware, certain attachments are blocked.
- Delete emails without opening from unknown and unexpected senders, especially emails with attachments and website links. Suspicious emails can be reported to SpamReview@HealthPartners.Com.
- All email sent externally from HealthPartners/GHI will have the footer systemically inserted:

“This email 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 email to the intended recipient, please be advised that you have received this email in error and that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited.

If you have received this email in error, please immediately notify the IS&T Support Center by
This policy applies to Group Health Plan, Inc. and all of its operating units and related organizations (collectively, “HealthPartners/ GHI”).

Email Address Forwarding and Blocking
- Email 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.

Email Access and Mobile Device Support
- External email access is allowed through Outlook Web Access (OWA) or Citrix applications. Two-factor authentication is required for remote email access.
- POP3 and IMAP protocols are prohibited and are blocked by HealthPartners/GHI email servers.
- Mobile devices with remote access let employees synchronize with the HealthPartners/ GHI email system.
- Corporate email can only be synced to a HealthPartners/GHI approved phone and only with approved Wireless Email Access software from the IS&T Desktop Standards list (MobileIron). It is prohibited to sync a HealthPartners/GHI approved phone to another phone or to sync to your personal accounts (i.e. personal folders, email, contacts, & calendars) and/or to use unapproved Wireless Email Access software for data synchronization to the HealthPartners/GHI network (MobileMe). Please note, it is acceptable to view your personal email from your phone, but prohibited to sync your HealthPartners/GHI email to your personal email account via your phone (can view personal email, but not sync it to work email).
- 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 email 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 email with Protected Information to ensure that the email recipient corresponds to the intended recipient. Any email 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 email using personal or web email programs (for example, Gmail, Hotmail, Yahoo or Comcast accounts).
- Do not send Protected Information via email to your personal email account(s).
- Use only an approved secure transmission method when sending Protected Information outside of the organization via email: Secure Email tool, E-transfer, TLS, or encrypted process performed by IS&T’s EDI team.
- Email messages containing Protected Information will not be forwarded to non-HealthPartners/GHI email addresses.
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 email, 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/Regions Hospital Purchasing Travel Card (PCARD) Program’s policy and procedures to send your cardholder account number via email.
3. In efforts to prevent identity theft, we strongly encourage you to not send your personal credit card numbers via email.

III. RISK

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

IV. DEFINITIONS

Email - The electronic transmission of information through an electronic mail protocol such as SMTP or IMAP. HealthPartners/GHI has standardized on Microsoft Outlook email client.

Encryption – a tool used to make information unreadable unless someone has a password.

Forwarded email – Email resent from an internal network to an outside point.

Chain email - 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 – Protected Health Information.

HIPAA – Healthcare Information Portability and Accounting Act.

IM – Instant Messaging. A real-time text messaging protocol.

Voicemail - includes messages that may be accessed directly from a phone as well as voice messages that are forwarded, stored and accessible through devices such as computers in any manner.

V. COMPLIANCE

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

VI. MONITORING AND MEASUREMENT

This policy will be reviewed every three years to determine its timeliness and relevance.

VII. 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/C1001

This policy applies to Group Health Plan, Inc. and all of its operating units and related organizations (collectively, “HealthPartners/ GHI”).
Using E-mail to Communicate With and About Patients and Members, Organizational Privacy Standard
Sending Protected Information Securely, Organizational Privacy Standard
HealthPartners/GHI Record Retention Policy