SCOPE: PeaceHealth employees, affiliated physicians, health care providers and their office staff, volunteers, vendors, students, contractors, and other individuals ("users") with access to PeaceHealth electronic mail (e-mail).

PURPOSE: To establish acceptable and unacceptable uses for PeaceHealth e-mail which include both internal and external e-mail.

POLICY: Users of PeaceHealth e-mail shall utilize the system in an ethical, lawful, respectful, and appropriate manner. E-mail messages are subject to other PeaceHealth policies, including those relating to harassment and discrimination.

REQUIREMENTS:

1. **Acceptable Uses.** Users of PeaceHealth e-mail shall utilize the system to promote the efficient and effective communication of PeaceHealth information. PeaceHealth allows personal use under limited circumstances.

   1.1. PeaceHealth supports personal use of e-mail to assist its employees in balancing their work and personal lives. Personal use during breaks and lunch periods is acceptable in accordance with appropriate use requirements. In addition, occasional personal use during work time may be conducted so long as it does not interfere with work performance, the operation of the department, or individual department policy.

   1.2. Users should consider that e-mail messages could be forwarded, intercepted, printed, and stored by persons other than intended recipients.

   1.3. Users will demonstrate the same care in writing and distributing e-mail as they would for other PeaceHealth communications. Communications are sent to recipients on a need-to-know basis, and sent with appropriate security measures applied. Encryption is required when sending confidential information, including protected health information, external to the PeaceHealth network. E-mail sent internally may be flagged as CONFIDENTIAL (message sensitivity) or have [secure] in the subject line of the message to notify the internal recipient that the message contains confidential information and will encrypt the message if it is forwarded externally.

   1.4. The following disclaimer is automatically appended to all external e-mail messages:

   "This message is intended solely for the use of the individual and entity to whom it is addressed, and may contain information that is privileged, confidential, and exempt from disclosure under applicable state and federal laws. If you are not the addressee, or are not authorized to receive for the intended addressee, you are hereby notified that you may not use, copy, distribute, or disclose to anyone this message or the information contained

herein. If you have received this message in error, immediately advise the sender by reply e-mail and destroy this message."

1.5. For PeaceHealth employees, students and volunteers, misdirected e-mail communications containing confidential information shall be reported using the incident reporting form on Crossroads under System-Wide Service Centers.

1.6. Third parties who use PeaceHealth e-mail are to notify the sender of misdirected e-mail communications containing confidential information.

1.7. E-mail distribution lists (dl's) are to be used for business purposes only.

2. **Unacceptable Uses.** PeaceHealth's e-mail shall not be used in a manner that is inconsistent with its mission and values, or violates PeaceHealth policies. Unacceptable uses include using e-mail to:

2.1. Engage in a use that interferes with the operation of PeaceHealth computer network services, with work performance, or the operation of a department.

2.2. Harass, stalk, intimidate, or threaten.

2.3. Access or transmit copyrighted materials, trade secrets, proprietary financial information, or confidential information, including protected health information without proper authorization and encryption.

2.4. Further unlawful or inappropriate uses such as commercial purposes, personal gain, or the advancement of individual views.

2.5. Bypass or breach security measures, or attempt to intercept an e-mail without proper authorization.

2.6. Impersonate another user or mislead a recipient about your identity.

2.7. Access or distribute obscene, sexually explicit, abusive, libelous, or defamatory material, in graphic or text form.

2.8. Solicit, initiate, or transmit chain e-mail, except as provided for by PeaceHealth and regional policies. E-mail will not be used for private or commercial business, benefit, or gain.

2.9. Engage in any other use that is determined to be contrary to the mission and values of PeaceHealth or violates of any laws or regulations.

3. **Protected Health Information (PHI) Requirements**

3.1. E-mail messages containing Protected Health Information (PHI) shall not be sent to anyone externally, unless the message is flagged as being CONFIDENTIAL (message sensitivity) or the message has "[secure]" in the subject line. The message subject line should never contain PHI. E-mail sent using these methods will be sent encrypted externally. E-mail messages sent internally using these methods will notify the internal recipient that the message contains PHI and will [secure] the message if it is forwarded externally.

3.2. **Clinician-Patient/Family E-mail.** E-mail sent between clinicians and their patients or patients' family members or others involved in the patients care, or between providers about their patients, shall be sent encrypted. PeaceHealth providers and patients communicating via e-mail on Patient Connection do not need to use encryption since PatientConnection is a secure web site.

4. **Quarantined E-mail.** All multi-media files (video and audio) are quarantined during delivery due to large storage and time requirements. Only PeaceHealth business and mission related multi-media files will be released. Personal multi-media files should not be sent (or attempted to send) or received and will not be released.

5. **Privacy Not Guaranteed.** All messages and documents created, sent, received, and stored in PeaceHealth e-mail are the property of PeaceHealth. PeaceHealth reserves the right to access and monitor electronic communications, including e-mail.

6. **Erasure Not Reliable.** Users should be aware that technologies for salvaging records can frequently make "deleted" records available for inspection. Therefore, users should not rely on the deletion of messages or documents to assume the message or document will remain private or confidential. E-mail documents are subject to discovery in legal proceedings to the same extent as hard copies. By transmitting a message via e-mail, a user may be deemed to have waived certain confidentiality protections that would otherwise be available. Users should carefully consider the confidentiality of the subject when determining whether to transmit the information electronically.

7. **E-mail Retention**

7.1. All contents of Outlook folders, including e-mail in the Inbox, Sent Items, Deleted Items, Personal Folders, Calendar, Notes, Tasks, and Journal, will be deleted 180 (one hundred eighty) days from the last modified date. The Contacts folder is not affected.

7.2. E-mail shall not be retained (or stored) in Public folders or shared mailboxes (RS:___) that are exempt from standard retention policy. Public folder and shared mailbox owners will be responsible for contents of their folders.

7.3. Users shall utilize alternatives for storing information contained in e-mails that will be deleted, such as word documents, text pad documents, etc.

7.4. Users shall not create or use personal storage containers (.pst) to store e-mail.

7.5. Backup tapes for Exchange e-mail servers are for disaster recovery only.

8. **Virus Controls**. Users shall not open attachments from unknown individuals, nor shall they attempt to deactivate automated virus control software on any computer.

9. **Violations.** Employees who engage in unacceptable practices while using PeaceHealth's e-mail system, or who violate policies relating to personal use, may be subject to corrective/disciplinary action up to and including termination of employment. Managers, in coordination with their Human Resources Department, are responsible for determining whether corrective/disciplinary action is required.

DEFINITIONS:

1. The term "*Confidential information*" refers to protected health information and information related to patients, other employees, providers, financial data, information protected by law, and other information pertaining to PeaceHealth unless specified otherwise.

2. The term "*External e-mail*" refers to e-mail sent outside the PeaceHealth network via the Internet.

3. The term "*Internal e-mail*" refers to e-mail sent within the PeaceHealth network.

4. The term "*Protected Health Information (PHI*)" refers to any individually identifiable health information (IIHI) relating to past, present, or future physical or mental health condition, provision of health care or payment for health care of an individual, created or received by PeaceHealth in any medium (written, electronic, or verbal).

5. The term "*third parties*" refers to affiliated physicians, health care providers and their office staff, volunteers, vendors, students, contractors, and other individuals with access to PeaceHealth electronic information systems.

REFERENCES:

Forms:
- PeaceHealth Electronic Incident Report

Job Aids & Tools:
- E-mail Encryption Procedures
- PeaceHealth Clinician E-Mail Communication Guidelines
- Public Folder Guidelines

Policy Documents:
- Policy #SYS.38.34 Confidentiality, Security, and Privacy of PeaceHealth Information

- Policy #SYS.38.37 Evaluation of Alleged Breaches of Confidentiality
- Policy #SYS.52.4 Harassment

HELP: For questions about this policy, or assistance with understanding your obligations under this policy, please contact the Human Resources Department, your local Desktop Representative, the Regional Privacy Officer, or the Technical Security Manager.

End of Policy

The final page of this document contains approval, review and revision information only.

ORIGINAL VERSION:

Author:	Tonya Erickson; Technical Security Manager		
Responsible Party:	Tonya Erickson; Technical Security Manager		
Reviewed By:			
Approved By:	Alan Yordy; President and CMO	**Date:**	7/23/2008

PERIODIC REVIEW:

Reviewer:		**Date:**	
Reviewer:		**Date:**	
Reviewer:		**Date:**	

REVISIONS:

Responsible Party:	Tonya Erickson; Technical Security Manager		
Revised By:	Tonya Erickson; Technical Security Manager		
Approved By:	SPOT	**Date:**	6/2/2011
Approved By:	Alan Yordy; President and CMO	**Date:**	6/2/2011
Reason/Summary of Changes:	General rewording under requirements.		
Replaces:			

RETIRED:

Requested By:			
Approved By:		**Date:**	
Reason for Retirement:			