Roswell Park Cancer Institute Policy and Procedure	Date Issued: 4/1/2000	Number: 905.1
Title: Email Use	Revision: 3	Effective Date: 1/6/14
Prepared by: Information Technology, General Counsel	Approved by: Michael B. Sexton, General Counsel	Page: 1 of 6

A. GENERAL STATEMENT OF POLICY

The purpose of this policy is to establish guidelines for the appropriate use of electronic mail by Roswell Park Cancer Institute (RPCI) employees, contractors, students or volunteers in communication with co-workers, patients, other health care providers or with the general public on or through RPCI owned computers, software and systems. Federal and New York State law and regulations governing the confidentiality of patient information must be complied with in any instance in which email is utilized to transmit patient medical or biographical information. Such information which has not been properly de-identified may only be transmitted to a non-Roswell email address through the use of encryption systems. Roswell currently employs Zix for user selectable email encryption and for private health information (PHI) content auditing - please see this link on the internal website for detail.

B. SCOPE

This policy and procedure applies to all members of the RPCI workforce.

C. ADMINISTRATION

This policy and procedure will be administered by the Vice President for Information Technology and Human Resources Department in consultation with the General Counsel.

D. POLICY / PROCEDURE

1. Email Risks. Although there are many benefits to communicating through the Internet, the informality of electronic communication can put an organization and its employees at legal risk.

    a. Legal Liability. RPCI may bear liability risks due to the content of information transmitted from its computer systems. Inappropriate emails can result in litigation against RPCI with the resultant risk of monetary judgments and penalties against the Institute. Information contained in emails may be damaging to the corporation, yet destruction or purging of such information once present may violate the law when there are pending lawsuits, audits or investigations. RPCI may be required to produce relevant email during discovery phases of litigation or during an investigation, or as requested under the New York Freedom of Information Law. Therefore, the email database should be clean of unnecessary messages. Regardless of retention in a specific mailbox, all emails after January 24, 2008 are kept in a permanent archive.

b. Confidentiality Breaches. Federal and New York State laws regulate the use and disclosure of protected health information (PHI). PHI must not be disclosed unless (i) the patient or his/her authorized representative has authorized the disclosure, or (ii) the disclosure is a necessary action in the ordinary course of treatment, billing, or hospital operations.

c. Damage to Reputation. The content of email reflects upon RPCI. A poorly written email or an email containing unprofessional or inappropriate content may expose the Institute to public ridicule, liability and/or damage to the Institute's reputation in the community.

d. Lost Productivity. Productivity is adversely affected by time spent on sending and receiving personal emails and unwanted SPAM messages.

e. Network Congestion and Downtime. Unnecessary email can cause Network congestion and can introduce harmful viruses into the computer system. RPCI has employed anti-spam and anti-virus systems to help reduce the volume of unsolicited and malicious email.

2. Ownership of Email. Email sent, received or stored on RPCI owned computers is the property of RPCI and is not private property of the computer user. RPCI Administration, through the President/CEO, VP of Human Resources or General Counsel, reserves the right to monitor incoming and outgoing messages and attachments and may disclose any electronic mail messages to law enforcement officials without prior notice to any employees who may have sent or received such messages. The IT Department and the VP of Corporate Ethics and Human Protection have the right to access any employee's mailbox as part of its investigatory function.

   A supervisor, with approval from department head, may also request that a certain user mailbox be opened if a department's business operations are affected due to a staff member's vacation, sick leave, or separation. This will allow work flow to continue. However, in general, any routine or scheduled departmental business process should not depend on a single user's mailbox. IT can offer assistance with reorganization when help is requested to open mailbox.

3. Guidelines for Work Related Use of Email by RPCI Staff.

   a. Patient Email. Electronic messages between active patients and RPCI clinicians and staff must be conducted through Patient Site. RPCI has developed Patient Site to comply with HIPAA Privacy and Security standards.

   b. Email Prescriptions. Patients often ask whether their medications may be prescribed over the phone or using email. Without being physically present with the patient, the prescribing physician could be prescribing medications to a person other than the appropriate patient; therefore prescriptions are not to be done over email and should only be done electronically via the Patient Site system.

   c. Email Emergencies. Email should never be used in an emergency situation, as there can be no guarantee that the intended recipient will receive the urgent message.

   d. Nationwide-Medical Practice. So-called " telemedicine", by which providers and the public communicate and exchange medical information, questions and advice through the internet and emails raises serious legal and liability issues, particularly where state lines are crossed. Currently there is no law uniformly

governing medical practice across state lines over electronic communication. Licensing, patient confidentiality, and malpractice issues may arise in these situations, with no clear conclusions to be drawn and with serious consequences such as allegations of unlicensed practice and loss of malpractice insurance coverage. **UNDER CURRENT NY LAW, TELEMEDICINE ACROSS STATE LINES IS TO BE AVOIDED**. While information can be exchanged with active patients, via Patient Site, new treatment relationships should not be established and maintained over the internet.

e. Protected Health Information and Email. PHI is health related or biographical information about a person, maintained by RPCI or Health Research, Inc. (HRI), relating to the past, present or future physical or mental health of the person, the provision of healthcare to the individual or payment for such healthcare by the person, and the information either identifies the person; or can be used to identify the person. For purposes of this policy, a recipient is considered to be a "permitted recipient" of PHI if the recipient meets the requirements of the RPCI governing the "minimum necessary" use or disclosure of PHI. PHI may only be transmitted via email if done in compliance with the following requirements:

   i. Internal Mail. PHI that may be used or disclosed legally may be transmitted to a permitted recipient through RPCI's internal network (intranet), provided the intended recipient is an authorized user of the RPCI intranet having an updated confidential access password to RPCI email. Note: only email addresses that end in roswellpark.org are "internal users." Be aware that some addresses that appear in the Outlook Global address list are not officially roswellpark.org addresses - these are easily distinguished by the globe Icon next to the name. When in doubt double click the "display name" of the addressee to display the underlying complete email address.

   ii. External Communications. PHI which is otherwise able to be used or disclosed, may be sent via email to an external permitted recipient over the internet only where encryption software is utilized to make the PHI non-distinguishable or non-readable in the absence of the corresponding decryption key, and such key is only held by authorized parties having confidential individual access passwords.

f. Email Redirection. Due to HIPAA regulations and the need to protect patient confidentiality, email redirection to an alternate email address will not be allowed. If a departing staff member is required to communicate using the Roswell email address for a period of time after he/she has left RPCI service, access will be granted for a limited time using the Email Web Access method with approval of supervisor. If this is desired, please submit a request to Human Resources.

g. Global or Broadcast Emails. All global emails to faculty and staff must be reviewed, approved, and disseminated by the Office of Public Affairs. Global emails are typically reserved for administrative communications that are urgent, time-sensitive and universally relevant. Please send prospective Global emails to Colleen Karuza, Director of Public Affairs, at Colleen.karuza@roswellpark.org for approval.

4. Guidelines for Email Administration

a. Mailbox Caps. The Institute's needs for Email storage has been dramatically increasing, which can negatively impact system performance. Each mailbox has a size limit. Mailbox owners are notified as storage is nearing the limit, so that appropriate steps can be taken to delete unnecessary emails and store important ones. Personal folders on local disk drives, shared departmental folders on centralized services or Home Directories are available to augment storage. It is especially important to use departmental shared folders for document collaboration rather than utilizing email services. Saving email and/or attachments to local folders is prohibited on non RPCI computers, laptops, PDAs, etc. Storage of sensitive data on local drives should be avoided and should be stored on departmental file servers or home directories. For many staff the need for or dependence on Personal Folders will diminish as production use of the email archive system increases.

b. Backup Retention. Each night, the IT staff creates a backup file of the email database. The backup file is maintained for 30 days for purposes of rebuilding mailboxes in the event of data corruption. Each mailbox owner is responsible for the backup and recovery of data in personal folders. Consult the IT Helpdesk for further instructions. All emails after January 24, 2008 are kept in a permanent separate archive.

c. Purge Email. Best business practice suggests deleting inactive or unnecessary email within 60 days. Moving messages to deleted items folder and purging folder does not permanently delete email from the system. All emails after January 24, 2008 are kept in a permanent archive. Each individual can retrieve archived mail by accessing https://emailarchive. The email archive is not an email system and does not substitute for the folder system in Exchange.

d. Attachment Storage. Where at all possible, do not store attachments within the email system. Documents accompanying messages that need to be saved should be separated from the email and maintained on a local disk drive in Home Directories or on a departmental shared server. Consult the IT Helpdesk for further instructions.

e. SPAM Filters. SPAM filters have been employed to reduce nuisance emails. SPAM filters do not eliminate all SPAM email. The daily SPAM summary report of email directed to junk mailbox should be reviewed for inadvertently diverted mail. For more information on spam management please see this link: http://tinyurl.com/cqvq4lx.

f. Virus Scanning. To protect our computing resources it is important that RPCI employs a comprehensive and vigilant approach to virus protection. RPCI scans each incoming message and attachment for viruses. Each time the virus software is updated the entire email database is scanned. Performance issues arise when this occurs because of the size of the database. This is not a perfect system therefore messages and attachments from unknown origins should not be opened.

5. Guidelines for Incidental Use of Email.

a. Incidental personal use of email by Institute employees, contractors, volunteers and students is to be kept to a minimum, subject to the following restrictions:

i. Incidental personal use of email must not interfere with the normal performance of an employee's work duties.

ii. No personal messages should be sent, received or saved that have a potential to expose the RPCI computer system to viruses or other harmful programs.
iii. To conserve space and network resources, employees should remove personal messages as soon as possible and not store such messages, attachments or files in the system.
iv. Inappropriate or prohibited email content, as described below, may not be included in email.
v. Except as noted above, it is a disciplinary offense to open an employee's email box without his or her permission or the permission of the Institute Counsel. An employee accessing another person's email in violation of this policy shall be subject to discipline up to and including dismissal in accordance with the collective bargaining agreement if applicable.

b. As a precaution against computer viruses, employees should not open unsolicited or unexpected email attachments without first confirming the contents of the attachment by checking with the sender. This is best handled by either calling the sender by phone or by sending a separate email to the sender to confirm that the message and attachment is not fraudulent.

6. Prohibited Content and Use.

a. The Institute could be exposed to liability or public ridicule due to the content in electronic communications by its employees. Therefore, employees must be vigilant to avoid content that could be construed as sexual harassment, discrimination, defamation, or infringement of another person's intellectual property rights (copyright, patent, trademark).

b. Trade secrets or other confidential information should not be transmitted through the internet without appropriate security pre-cautions.

c. Employees may not distribute materials through email that solicit for or otherwise promote outside organizations, religious and/or political positions, or personal business activities without administrative approval.

d. Chain letters, written or electronic, using internet, email or inter-office mail are not permitted at the Institute and should be deleted.

e. Employees should not use email for purposes of political lobbying or campaigning.

7. EMAIL DISCLAIMER. An appropriate disclaimer will automatically be placed on all emails sent outside of Roswell Park.

8. POLICY VIOLATIONS. Any violations of this policy will be addressed through the progressive disciplinary process in accordance with the collective bargaining agreements, if applicable.

9. COMPLIANCE. Audits for HIPAA Violations will be performed by IT Security on a bi-monthly basis. IT Security will present the findings to the IT Advisory Board for guidance and/or resolution. Every effort will be made to prevent audits from causing operational failures or disruptions.

10. SANCTIONS. Violations of this policy will be addressed through the corrective counseling and/or progressive discipline process in accordance with the collective bargaining agreements, if applicable.

E. DISTRIBUTION

This Policy and Procedure will be distributed to all Institute Managers via the RPCI internal web page and to holders of backup hard copies of the manual. Managers are responsible for communicating policy content to pertinent staff.