



Chief Executive Officer of the Medical Center

MEDICAL CENTER POLICY NO. 0193

- A. SUBJECT: Electronic Mail (E-mail)
- B. EFFECTIVE DATE: April 1, 2016 (R)
- C. POLICY:

1. Applicability

Electronic mail (e-mail), when used properly, can be an effective tool for communication of business information. It is not advisable to use e-mail for confidential information or when there would be concern if the e-mail were forwarded to other parties, or if all or some portion were to be copied and sent to other parties. Confidential information includes, but is not limited to, protected health information, employee information, and financial information.

E-mail can be subject to discovery in litigation and may be subject to a Request for Information under the Freedom of Information Act.

The Medical Center maintains a computer network, the Secure Clinical Subnet, which includes a "firewall" between it and the Internet. This firewall provides a measure of security against external threats, but is not invulnerable. Many departmental and School of Medicine e-mail systems are outside this firewall, and thus are more vulnerable.

E-mail accounts protected behind the firewall are displayed in the Global Address Book with an *HS added after the name. E-mail sent to an account that appears in the Global Address Book with an *HS, may include identifiable patient information such as the patient's name or medical record number if necessary. See [Medical Center Policy No. 0201 "Patient Identification"](#) regarding patient identifiers.

The e-mail usage practices at the University of Virginia Medical Center as outlined in this policy shall be followed to promote maximum privacy and security of confidential information. This policy applies to those within the University of Virginia Health System using the Medical Center's Exchange server (*HS).

2. General Usage Requirements

- Medical Center e-mail systems are to be used for Medical Center business purposes. Outside e-mail systems such as Gmail, Hotmail, Yahoo, AOL, other academic institutions' systems, etc., shall not be used for any Medical Center purposes. E-mail may not be auto-forwarded to other e-mail systems.

(SUBJECT: Electronic Mail (E-mail))

- *HS accounts are available to Medical Center employees, clinical staff and University employees to transmit or receive patients' protected health information.
- Accounts must be terminated when an employee or clinical staff member leaves the Medical Center.
- Limited personal use of e-mail is acceptable only if it does not impede business functions or consume excessive institutional resources.
- E-mail used for business purposes unrelated to the Medical Center is prohibited and may result in termination of e-mail account and other disciplinary measures.
- The content of Auto Signatures shall be limited to the sender's identifying information (name, credentials, title and contact information). Additional superfluous content (i.e., quotations, phrases) is prohibited.
- Persons with e-mail accounts shall safeguard their passwords and shall not reveal them to others. In HSTS administered systems, HSTS is unable to recover a forgotten password; it can only change the password to a new, known value. See [Medical Center Policy No. 0163 "Access to Electronic Medical Records and Institutional Computer Systems"](#) for access and security policies.

Guidelines for Use of e-mail are posted on the Health System Technology Services (HSTS) website at:

<http://www.hsts.virginia.edu/procedures/email-account-standard>

E-mail shall not be used to transmit any potentially offensive, disruptive or harassing materials (i.e., items containing sexually suggestive content, racial slurs, obscene material or any other comments or content that offensively address age, gender, sexual orientation, religious or political beliefs, national origin or disability).

Also prohibited are:

- Sending advertisements for games of chance;
- Sending chain letters (i.e., non-business related e-mails intended to be repeatedly forwarded to lists of e-mail accounts).

3. Provider/Patient Communications

Rather than using e-mail, patients should be encouraged to use MyChart, which provides a more secure and reliable provider/patient means of electronic communication. MyChart is available at <https://mychart.healthsystem.virginia.edu/mychart/>. Providers who plan to use e-mail with their patients shall follow the guidelines posted on the Health System Privacy Office web site at <http://www.medicalcenter.virginia.edu/intranet/ccpo/privacy-office/privacy-guidelines>

4. Administrative Monitoring

HSTS monitors system performance and resources of the e-mail system. SPAM and excessive non-work related List-serve mails place an unnecessary load on the e-mail system that may affect

(SUBJECT: Electronic Mail (E-mail))

performance and consume valuable resources.

If an e-mail system or address is suspected of abuse or is otherwise not in compliance with this policy, HSTS may take immediate action, including blocking any e-mail messages being sent from the suspected e-mail system or address.

All e-mail traffic may be monitored for compliance with HIPAA, HITECH, and other Federal and Commonwealth privacy and security regulations. With senior management approval, individual e-mail accounts may also be accessed for personnel, technical or administrative reasons. Any violations of law, regulation, and/or Medical Center policies will be addressed on a case by case basis.

5. Mail System Integrity

E-mail system integrity can be compromised by computer viruses, excessive mailings of large notes or file attachments, and by inadvertent or intentional attempts to damage or delete system files.

Immediate action, including immediate termination of a user's account without warning, will be taken if the integrity of the e-mail system is threatened.

6. Mass Mailings for Business Purposes

Large mailings quickly saturate an e-mail system if used too frequently. HSTS will accept only notices of wide interest to the Medical Center community for mass mailings sent to all Medical Center e-mail customers, such as:

- Downtime notices for computer systems;
- Events held at the Medical Center conducted for the benefit of Health System employees;
- Health and safety notices to the general community;
- Notices forwarded from Medical Center or University of Virginia Executive staff.

Mailings intended for mass distribution must be approved by HSTS based on administrative guidelines found at the following URL:

<http://www.hsts.virginia.edu/procedures/health-system-mass-email-broadcast-email>

Requests for mass mailings shall be forwarded to the HSTS Help Desk. HSTS will review the content and, if deemed appropriate, will perform the mailing usually within a 48-hour period. If the mailing is rejected, or a more limited mailing is approved, the requesting person will be notified.

D. PROCEDURE

1. Always double-check addresses before sending e-mail.
2. Delete confidential e-mail when finished.

(SUBJECT: Electronic Mail (E-mail))

3. If e-mail will be distributed to the same group on a regular basis, consider establishing a secure closed shared drive location where the group can access information outside of e-mail. E-mail messages can then be used to notify the group of new data on the secure site.
4. Ensure that any PC accessing the network (e.g. a home computer using the VPN) has current antivirus files and security patches.
5. Use a confidential flag on e-mail containing confidential information and/or create a confidentiality notice on the message, such as the sample provided immediately below.
However, be aware that while labeling a document as confidential or privileged may help guide recipients, it may not protect from legal process (e.g., a subpoena) or Freedom of Information Act demand, nor will it mitigate or avoid the consequences of an intentional or unintentional HIPAA breach.

The following is a sample e-mail confidentiality notice from the AMA Guidelines:

“E-mail Confidentiality Notice

The information contained in this e-mail is confidential, privileged, or otherwise protected from disclosure. It is intended only for the use of the authorized individual(s) as indicated in the e-mail. Any unauthorized disclosure, copying, distribution or taking of any action based on the contents of this material is strictly prohibited. Review by any individual other than the intended recipient does not waive or give up the physician-patient privilege. If you have received this e-mail in error, please delete it immediately and notify the sender.”

7. Mail Storage: Preservation of E-mail in Litigation; Restoration of E-mail
 - a. Each e-mail user should monitor his/her saved mail and periodically purge or archive it to insure that all e-mail users have adequate storage available for their e-mail messages.
 - b. The owner of any e-mail account with excessive storage will be contacted and asked to remove or archive a percentage of his/her e-mail.
 - c. If litigation relevant to the subject matter of a particular e-mail or series of e-mails has been or reasonably appears likely to be commenced the user should promptly take steps, in consultation with HSTS, legal counsel, and Patient Safety and Risk Management, to identify and preserve all relevant e-mail messages.

Should employees require restoration of deleted e-mail, approval by their Administrator is required.

Procedure for restoration is at:

<http://www.hsts.virginia.edu/procedures/email-and-file-restoration-and-email-access-approval>

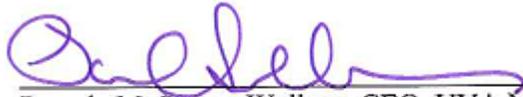
8. Termination of Accounts
 - a. Upon the effective date of separation of employment or receipt by HSTS of notification of termination, whichever is later, HSTS shall, as expeditiously as possible, disable the employee's account and remove the employee's entry in the Global Address List (GAL).

(SUBJECT: Electronic Mail (E-mail))

Separated employees' account will be permanently deleted after being disabled unless approval for continuation is granted per 8.c.

- b. No later than 30 days following the termination date, the separated employee's supervisor/manager may request that the contents of the folders to be transferred to such supervisor/manager's account.
- c. Permission can be granted to a separated employee for continuation of his/her HSTS e-mail account to continue conducting official health system business. All requests for continued access shall be made in writing at least two weeks prior to separation from employment to the Chief Information Technology Officer (CITO) or designee, who shall notify and consult with the senior administrator or department chair of the applicable area to validate the business need for continued e-mail use. Requests shall be granted on a case-by-case basis at the sole discretion of the senior administrator or department chair of the applicable area.

SIGNATURE:



Pamela M. Sutton-Wallace, CEO, UVA Medical Center

DATE:

3/22/2016

Medical Center Policy No. 0193 (R)

Approved November 1997

Revised July 2000, November 2002, December 2003, September 2005, September 2006, December 2009, June 2011, March 2013, March 2016

Approved by Chief Information Technology Officer

Approved by Medical Center Administration