Rancho Los Amigos National Rehabilitation Center

ADMINISTRATIVE POLICY AND PROCEDURE

SUBJECT: ELECTRONIC MAIL (E-MAIL)

Policy No.: A300.1
Supersedes: May 2009
Revision Date: December 3, 2015

PURPOSE:

The purpose of this policy is to protect the security, confidentiality, and integrity of health information contained in electronic mail (e-mail) as required by law, professional ethics, and accreditation requirements.

POLICY:

This policy defines guidelines for the appropriate use of e-mail and applies to all employees (defined as full or part-time, temporary or permanent, medical staff, contractors, students, agency personnel, registry, interns, volunteers, and others) who are authorized to read, enter, or update information created or transmitted via e-mail (hereinafter referred to as "users"). This policy further applies to all usage of the e-mail system where the mail either originated at Rancho or from an external mail system.

Each user at Rancho shall understand and abide by this policy and sign the Computer Security and Protected Health Information Guidelines (A300) and Electronic Mail (A300.1) Acknowledgment (Attachment 1) on an annual basis, a copy of which will be included in the Official Personnel Folder.

Assumptions

- E-mail can be immediately broadcast worldwide and received or intercepted by many intended and unintended recipients.
- Recipients can forward e-mail messages to other recipients without the original sender's permission or knowledge.
- Users can easily misaddress e-mail.
- E-mail is easier to falsify than handwritten or signed documents.
- Backup copies of e-mail may exist even after the sender or the recipient has deleted his or her copy.
- An e-mail containing information about a patient's diagnosis and/or treatment constitutes a part of the patient's medical records and is Protected Health Information under the Federal Government's Health Insurance Portability and Accountability Act (HIPAA).

PROCEDURES:

1. Expectations of Privacy

The e-mail system and all messages generated or handled by e-mail, including backup copies, are part of the business equipment of Rancho Los Amigos, are owned by the County of Los Angeles, and are not the property of the users of the system. Management reserves the right to review e-mail

APPROVED BY:
Signature(s) on File.

messages under the following conditions: retrieving data in an employee's absence, preventing excessive personal use of business equipment, and violations of company rules and policies. All e-mail messages are automatically stored on the server's backup system, and the delete message function does not restrict or eliminate management's ability to retrieve and review e-mail.

2. Right to Monitor, Audit, Delete, Read

The County of Los Angeles reserves the right to monitor, audit, and read e-mail messages. The County of Los Angeles may monitor content and usage of e-mail messages to support operational, maintenance, auditing and compliance to policies, security, and investigative activities.

3. Prohibited Uses

Rancho's e-mail system may not be used for any purpose other than County business. Use of e-mail accounts for personal business may result in disciplinary action. E-mail messages are considered legal documents.

a. Statements shall not be made on an e-mail that would not be appropriate in a formal memo.
b. Users must not transmit confidential or proprietary information to unauthorized recipients. Proprietary information is information that belongs to the County of Los Angeles.
c. Users must not transmit obscene, offensive, harassing, or hostile messages to any recipient. Users shall not enter, transmit, or maintain messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition. Users shall not enter, maintain, or transmit any abusive, profane, or offensive language.
d. Users must not transmit information that is protected by the attorney-client privilege, e.g., information related to a lawsuit or investigation.
e. E-mail transmissions must not involve any illegal or unethical activity.
f. E-mail transmissions must not involve solicitations unrelated to County business. Users may not use Rancho's e-mail system to solicit for outside business ventures, organizational campaigns, or political or religious causes.
g. Users must not use e-mail to transmit highly confidential or sensitive information, e.g., discussion of HIV status, mental illness, chemical dependency, and workers compensation claims.
h. Users must not use e-mail addresses for marketing purposes without explicit permission from the target recipient.
1. Users must not share professional e-mail accounts with family members.

4. Patient, Confidential or Sensitive Information

a. Rancho Los Amigos will make all e-mail messages sent or received that concern the diagnosis or treatment of a patient part of that patient's information and will treat such e-mail messages with the same degree of confidentiality as other pieces of patient information.
b. All e-mail concerning patient information will start with a banner stating that this is a confidential medical communication (see below).

This is a CONFIDENTIAL Medical Communication
If you have received this information in error,
please notify the sender immediately and arrange for the return
or destruction of this message and its attachments.

c. The Provider's e-mail "signature" shall contain the provider's contact information, e.g., telephone number, fax number, and address.
d. Users must double check all "To" fields before sending messages.
e. All e-mail communications containing patient, confidential and/or sensitive information to someone outside of the County's e-mail system must be encrypted to comply with State and federal privacy laws and DHS policies. E-mail addresses outside of the County's e-mail system include any that do not end with".lacounty.gov"
- Send the recipient an un-encrypted e-mail notifying them they will be receiving an encrypted e-mail with instructions to follow on how to open it.
- You must add the word "Secure" in square brackets on the in the subject line of the e-mail to encrypt it. For example Subject: [Secure] Nursing Home Placement for Rancho Patient

f. E-mail concerning the diagnosis or treatment of a patient constitutes a form of the progress note. It is the responsibility of the provider to indicate the patient's name and medical record number in the correspondence. The provider shall print in full each e-mail message and place a copy in the patient's medical record or send a copy to Health Information Management for placement into the patient's medical record.
g. Printers must operate in an area that is accessible to staff only and not to patients.
h. E-mail correspondence with a patient containing protected health information must be approved by the patient's signature on a release form. Contact the Health Information Management department for the proper consent form.

5. User Security
The e-mail system must employ user-IDs and associated passwords to isolate the communications of different users. Employee password protection on e-mail does not provide a special right of privacy to the employee. Password protection is given only to prevent other employees and third parties from accessing the employee's communications and does not protect the employee from access by the Employee's Supervisor or Department Head. Users must never share passwords or reveal them to anyone else. If users must share data, they must use the message-forwarding function. Users may not intercept, disclose, or assist in intercepting and disclosing e-mail communications.

6. Forwarding E-Mail
Because some information is intended for specific individuals and may not be appropriate for general distribution, users should exercise caution when forwarding messages.

7. Everyone E-Mail Messages
Users are restricted from addressing messages to "Everyone" without prior approval from the Rancho Public Improvement Officer (PIO) Approval may be obtained by completing and submitting the "Everyone E-Mail Approval Form" which is found on the Intranet under Forms/Employee Forms/Administration/Everyone E-Mail Approval Form.

8. Purging E-Mail
Users should periodically purge from their personal e-mail storage areas messages that are no longer needed for business use. E-mail messages located in personal e-mail storage areas (i.e., message inbox) that are three years old or older will be automatically deleted. Items in outbox that are over

six months old will be automatically deleted. (Messages in Trash will be deleted every 3-monthst) to maintain e-mail system stability and integrity. With Outlook, there is no longer an Archive tool.

9. Attachments to E-Mail and Protected Health Information

All attachments to e-mail containing protect protected health information must not be sent outside of DHS (any that do not end with ".lacounty.gov") unless the attachment is encrypted per instructions on item 4.e of page 3 above. Contact Information Management Services, Operations Manager via the Help Desk at extension 4357, for help, if, necessary.

10. Reporting Requirements

Users must immediately report any violations of this Policy to their Supervisor. Failure to do so constitutes a violation of this Policy.

11. Enforcement

Supervisors are responsible for enforcing this policy. Users who violate this policy are subject to progressive discipline, up to and including termination from employment, and/or criminal prosecution.

Attachments: Attachment 1 - Acknowledgment of Computer Security Guidelines (Policy A300) and Electronic Mail (policy A300.1)
Attachment 2- Everyone E-Mail Approval Form

References:

Computer security guidelines, administrative policy A300, June 2000.

Kane B and Sands DZ. Guidelines for the clinical use of electronic mail with patients. Journal of the American Medical Informatics Association (JAMIA). 1998; 5: 104-111.

Sands DZ. Guidelines for the use of patient-centered e-mail. Massachusetts Health Data Consortium. 1999. (http://www.mahealthdata.org/mhdc/).

Tomes J. Adopt e-mail policy to protect confidential information. Health Information Compliance Insider. July 2001; 1-5.

Cross References:

DHS Policies:	361.8	Minimum Necessary Requirements for Use and Disclosure of Protected Health Information (PHI)
	935.20	Acceptable use Policy for County Information and Technology Resources
Rancho Policies:	A300	Computer Security and Protected Health Information (PHI) Guidelines, administrative policy, revised May 2007.
	A331	Computer Workstation Use and Security
	A334	Privacy and Security Awareness and Training

FT:ad

Rancho Los Amigos National Rehabilitation Center

Computer Security and Protected Health Information Guidelines (A300) and Electronic Mail (A300.1)

I understand it is the policy of Rancho Los Amigos National Rehabilitation Center (RLANRC) that all personnel (defined as employees, contractors, students, agency personnel, volunteers, whether they are permanent, temporary, part-time, or other) are personally responsible for the protection of all RLANRC information, HIPAA-related protected health information, data, and information processing resources which they have access to by virtue of employment by RLANRC.

I hereby acknowledge being responsible for the proper use of electronic equipment and the privacy, integrity and availability of RLANRC data in compliance with RLANRC Computer Security and Protected Health Information (PHI) Guidelines Policy (A300) and Electronic Mail (A300.1).

ACKNOWLEDGMENT

By signing where indicated below, I acknowledge and affirm each of the following:

1. I have received and carefully reviewed a copy of RLANRC Computer Security and Protected Health Information (PHI) Guidelines Policy (A300) and Electronic Mail Policy (A300.1).

2. I understand that I shall be held personally responsible and accountable for complying with these policies.

3. I am aware that if I violate any provisions of these policies, I will be subject to disciplinary action that may include discharge from service, and/or agency.

EMPLOYEE NAME (PRINT)	EMPLOYEE NO.
SIGNATURE	DATE
SUPERVISOR'S NAME (PRINT)	
SUPERVISOR'S SIGNATURE	DATE

Distribution: Original - Employee Official Personnel Folder, Copy- Employee, Copy- Departmental Area File