Children’s Hospital Los Angeles Medical Group

Compliance Policy Manual

Policy	HIPAA Privacy & Security – E-mail & PHI
Sign Off	Robert Adler, M.D., CHLAMG Compliance Officer
Issued	June 1, 2013
Revised	June 11, 2018
Number	CHLAMG 10-0007

Background

Electronic mail or e-mail is a potential high-risk area for improper disclosure of confidential information, especially for those containing protected health information or PHI. When staff use e-mail prudently, it can greatly increase the level of communication and productivity for a management services organization. But when people use e-mail improperly, it can represent significant risk to the patient’s right to confidentiality leading to potential legal and ethical dilemmas. The HIPAA Security Rule mandates that covered entities develop and implement policies and procedures to safeguard ePHI.

Policy

Patient Communication

Pediatric Management Group (PMG) will be responsible for following these rules regarding the acceptable use of e-mail for patient communication:

- Documenting procedures that ensure e-mails include headers at the top of all patient e-mail communication. For example:
  “This message contains CONFIDENTIAL medical communications. If you are not the intended recipient, please discard the message immediately and inform the sender that the message was sent in error.”

- Documenting procedures that ensure ALL e-mail communication contains a disclaimer at the bottom of the message. For example:
  “Confidentiality Notice: This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.”

General E-mail Use Requirements

Staff members shall be responsible for complying with the following requirements:

1. PMG does **NOT** permit staff to use personal e-mail accounts (AOL, Comcast, Hotmail, etc.) for communicating ePHI. All PMG employees that require the use of e-mail to communicate ePHI must do so through a PMG managed e-mail account.

2. Resolve request from patients, referring physicians, or other business associates to discuss information not appropriate for e-mail via telephone, fax or in person. Do **NOT** communicate the following information via e-mail:
   – Protected diagnoses (i.e. mental health, substance abuse, HIV/AIDS)
   – Workers compensation injuries and disability
   – Confusing or abnormal test results
   – New diagnosis

- Bad news
- Anything urgent
- Any statements you would not make speaking to the patient over the telephone.

It is the intention of PMG in conjunction with CHLA Information Systems to implement a secure messaging system to provide secure e-mail communications with patients and referring physicians. PMG in conjunction with CHLA shall create, document, implement, and maintain procedures for the following:

Use of a secure messaging system to communicate ePHI
Secure messaging systems must minimally be able to provide the following:

- Confidentiality of the information people exchange
  - If the message is sent over an open network (e.g. the Internet), it must be encrypted using an encryption standard approved by the Security Officer.
  - To encrypt an e-mail message, click FILE → PROPERTIES → SECURITY → ENCRYPT. Contact the IT Help Desk if you need more information.
- Refer to the CHLA Information Systems Help Desk for full details of the HIPAA-HITECH Security and Privacy requirements.

RESOURCES

Federal Law: 45 CFR §§ 164.312(e)

Policy CHLAMG 10-0006 HIPAA Compliance