CHILDREN'S HOSPITAL LOS ANGELES MEDICAL GROUP
COMPLIANCE POLICY MANUAL

POLICY	HIPAA Privacy
SIGN OFF	Robert Adler, M.D., CHLAMG Compliance Officer
ISSUED	April 14, 2010
REVISED	May 22, 2018
NUMBER	CHLAMG 10-0006

PURPOSE

To ensure that Children's Hospital Los Angeles Medical Group (CHLAMG) maintains patients' Protected Health Information (PHI) in medical and business records in a confidential manner consistent with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

HIPAA Privacy Compliance: The HIPAA Privacy Rule requires that workforce members adhere to controls and safeguards to: (1) ensure the confidentiality, integrity and availability of confidential information; and (2) detect and prevent reasonably anticipated errors and threats due to malicious or criminal actions, system failure, natural disasters and employee or user error.

SCOPE

Who is subject to HIPAA? HIPAA regulations apply to all employees, health care providers, trainees and volunteers at CHLAMG and its Affiliates; Pediatric Management Group, LLC, (PMG); Pediatric and Adolescent Hematology Oncology (PAHO); and affiliated health care sites or programs. HIPAA regulations also apply to anyone who provides financial, legal, business or administrative support to CHLAMG and its affiliates.

DEFINITIONS

Covered entity: CHLAMG and affiliates; Pediatric Management Group, LLC and Pediatric and Adolescent Hematology Oncology (PAHO), hereinafter referred to as CHLAMG.

Business Associate: A person or entity in a contractual relationship with a covered entity to perform services for treatment, payment or operations.

Individually Identified Health Information (IIHI): Health data of patients that includes the patient name, address, social security number, health plan coverage, diagnosis, treatment, and other special circumstance data such as psychiatric, HIV, or sexually transmitted disease/reproductive status information.

Protected Health Information (PHI): PHI is IIHI that is attributable to a specific patient. Covered entities—including health care providers, health plans, or clearinghouses--create, receive, and transmit PHI. PHI may exist in different forms or mediums, such as verbal communications.

Triad of Operations: The Triad of Operations includes the three activities for which CEs may use or disclose PHI without the patient's authorization: Treatment, payment for services, and health care operations.

Minimum necessary standard: To provide the least amount of information necessary to complete a task.

De-identification: The removal of identifiers to prevent accidental disclosure of a patient and their diagnosis or treatment.

PERMITTED USES AND DISCLOSURES

Employees of CHLAMG may use or disclose PHI for the following purposes without the patient's (or their family's) authorization.

1. Internally for treatment, payment, and health care operations (TPO)

2. To share with another covered entity for business, legal, financial, or administrative purposes working on behalf of CHLAMG, such as collection agencies, financial auditors, or attorneys. Some other examples include:
    - Conducting quality assessment and improvement activities
    - Developing clinical guidelines
    - Conducting patient safety activities as defined in applicable regulations
    - Conducting population-based activities relating to improving health or reducing health care cost
    - Developing protocols
    - Conducting case management and care coordination (including care planning)
    - Contacting health care providers and patients with information about treatment alternatives
    - Reviewing qualifications of health care professionals
    - Evaluating performance of health care providers and/or health plans
    - Conducting training programs or credentialing activities
    - Supporting fraud and abuse detection and compliance programs.

    In general, before a CE can share PHI with another CE for one of the reasons noted above, the following three requirements must also be met:
    1. Both CEs must have or have had a relationship with the patient (can be a past or present patient)
    2. The PHI requested must pertain to the relationship
    3. The discloser must disclose only the minimum information necessary for the health care operation at hand.

3. To share with the Department of Health and Human Services (DHHS) to investigate compliance with HIPAA policies. Forward any such request to the Compliance Department.

4. Services related to government or public health activities. Forward requests to the Compliance Department

PROCEDURE

CHLAMG requires, without exception, that all employees keep the PHI of our patients confidential. Staff must adhere to the following: (note any reference below to "desktop" or "workstation" refers to any electronic device, e.g., laptop, tablet, etc., that can access and display PHI)

1. Do not discuss patient information with co-workers, unless they have a need to know to do their work. It is your responsibility to protect the information of your patient(s).
2. When seeking guidance or clarification, use the "minimum necessary rule" to achieve your goal. In other words, provide only that level of information necessary to complete the task. For example, if you have a question regarding a code, there should be no reason to state the patient's name in order to assign the correct code.
3. Do not remove any non-encrypted files from the hospital campus or clinics that contains PHI. This includes sending non-encrypted e-mail to unauthorized sources and sharing information with others who are not members of a covered entity (and do not have a need to know) verbally.
4. Do not remove any non-encrypted device from the hospital campus or clinics that contains PHI, without the express written consent of the Compliance Director. This includes lap tops, jump drives, or other electronic storage device.
5. Do not forward any PHI from your work computer to an external email address, including your personal email addresses.
6. Do not fax PHI to an unrestricted fax number. You must confirm that the business associate receiving the information has a secure fax line prior to submitting the information.

7. Always use a fax coversheet (once a secure fax line has been determined) that warns the recipient that the attached fax includes PHI, and that if they do not have authorization to view the information, that they should either destroy the information, or return it to the sender.
8. Never leave your work station without closing down active screens displaying PHI.
9. All desktop computer programs with access to PHI must be password protected.
10. Lock your desktop computer when you leave your work station (i.e. ctrl+alt+del – click on "lock" button or invoke a password protected screen saver)
11. Use a screen saver that automatically shuts the screen down after a reasonable period of non-activity for all desktop computers and requires your password to log back in.
12. Never share your work password with anyone.
13. Submit all subpoenas or requests for PHI to the Compliance Director.

For all other instances, seek clarification from your Department Manager or the Compliance Department. If in doubt, do not disclose.

VERIFICATION OF IDENTITY

The Privacy Rule requires covered entities to verify the identity and authority of a person requesting protected health information (PHI), if not known to the covered entity. See 45 C.F.R. § 164.514(h). The Privacy Rule allows for verification in most instances in either oral or written form, although verification does require written documentation when such documentation is a condition of the disclosure.

The Privacy Rule generally does not include specific or technical verification requirements and thus, can flexibly be applied to an electronic health information exchange environment in a manner that best supports the needs of the exchange participants and the health information organization (HIO). For example, in an electronic health information exchange environment:

- Participants can agree by contract or otherwise to keep current and provide to the HIO a list of authorized persons so the HIO can appropriately authenticate each user of the network.
- For persons claiming to be government officials, proof of government status may be provided by having a legitimate government e-mail extension (e.g., xxx.gov).
- Documentation required for certain uses and disclosures may be provided in electronic form, such as scanned images or pdf files.
- Documentation requiring signatures may be provided as a scanned image of the signed documentation or as an electronic document with an electronic signature, to the extent the electronic signature is valid under applicable law.

VIOLATIONS

If you witness something that causes you to question the appropriateness of a release of PHI, call the incident to the attention of your Department Manager, Director, Compliance Department, or the anonymous, confidential HOTLINE at (877) 658-8022. This call is toll-free. CHLAMG has a non-retaliation policy for complaints.

REFERENCES

For more information about HIPAA regulations, you may access the complete Privacy Rule on the Office of Civil Rights at the Department of Health and Human Services website: http:\\www.hhs.gov/ocr/hipaa.

Policy CHLAMG 15-0012 Responding to External Requests for Information

Policy CHLAMG 10-0008 HIPAA Privacy and Security Enforcement Training

Policy CHLAMG 10-0007 HIPAA Privacy and Security, E-Mail

Policy on Social Media and Personal Devices *see Code of Conduct