Children's Hospital LOS ANGELES Medical Group	POLICY AND PROCEDURES		
	POLICY NUMBER:	CHLAMG-CI-1011	
	ORIGINAL DATE: 4/14/2010	REVISED: 11/2/2018	EFFECTIVE: 12/26/2018
DEPARTMENT: Compliance	APPROVED BY: Carl Grushkin, MD and Chief Compliance Officer		
POLICY TITLE: **Protection of Patient Health Information and other Confidential Information**			

PURPOSE:

To ensure that Protected Health Information (PHI) contained within the medical and business records of Children's Hospital Los Angeles Medical Group (CHLAMG) is maintained in a confidential manner consistent with Health Insurance Portability and Account (HIPAA) Act Privacy Rule and California law relating to the confidentiality of medical information.

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:

This policy applies to all CHLAMG workforce members which include 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. The HIPAA Privacy Rule and its requirements also apply to anyone who provides financial, legal, business or administrative support under a Business Associate Agreement to CHLAMG and its affiliates.

DEFINITIONS:

Business Associate: Includes a health information organization, e-prescribing gateway or other person that provides data transmission services with respect to protected health information to CHLAMG and requires access on a routine basis to such protected health information; a person that offers a personal health record to one or more individuals on behalf of a covered entity; and, a subcontractor that creates, receives, maintains or transmits protected health information on behalf of the business associate.

Disclosure: Means the release, transfer, provision of access to, or divulging in any manner of information outside of the CHLAMG entity holding the information.

Health Care Operations: Refers to a broad range of activities including quality assessment, patient education and training, student training, contracting for health care services, medical review, legal services, auditing functions, compliance, business planning and development, licensing and accreditation, business management and administrative services.

Individually Identified Health Information (IIHI): Is information that is a subset of health information, including demographic information collected from an individual, and: (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present or future physical or mental health condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual.

Minimum necessary standard: The requirement to use the minimum necessary amount of protected health information for routine uses, disclosures and requests. The minimum necessary standard does not apply to treatment, disclosures to the individual of his or her own PHI, disclosures pursuant to an individual's authorization, disclosures to HHS for enforcement purposes, and uses and disclosures that are required by law, but does apply in other circumstances.

Payment: Refers to activities relating to activities to obtain or provide reimbursement for the provision of health care. Examples of payment activities include determinations of eligibility or coverage; billing, claims management, collection activities; review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; utilization review activities; disclosure for payment activities of another covered entity or health care provider.

Protected Health Information (PHI): Means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium (paper, oral, etc.). Protected health information excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), employment records held by CHLAMG in its role as an employer; and records relating a person who has been deceased for more than 50 years.

Treatment: Means the provision, coordination, or management of health care and related services by one or more health care providers, including coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Use: Means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within a CHLAMG entity that maintains such information.

POLICY:

CHLAMG considers all information regarding patients as confidential. PHI, which includes demographic and medical information, may only be used and disclosed in accordance with state and federal laws and this policy. For uses and disclosures other than Treatment, Payment and healthcare Operations ("TPO"), disclosures to the patient or patient's personal representative, and disclosures permitted or required by law, an authorization is required. If you are uncertain about a use or disclosure of PHI, you should request assistance from a supervisor or the Compliance Department.

For disclosures to a CHLAMG business associate, a fully executed Business Associate Agreement using the approved CHLAMG template is required prior to any such disclosure.

Workforce members and business associates who use and disclose PHI are responsible for taking appropriate precautions to prevent unauthorized access to PHI during daily operations.

PROCEDURE:

Without exception, all CHLAMG workforce members are required to keep PHI confidential. The following requirements apply:

1. **Minimum Necessary Standard**. All CHLAMG workforce members must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. This requirement does not apply to:

    a. Disclosures to, or requests by, a health care provider for treatment;
    b. Uses or disclosures made to the patient or patient's personal representative;
    c. Uses or disclosures made pursuant to the patient's (personal representative's) valid authorization;
    d. Disclosures made to the Secretary of the U.S. Department of Health and Human Services (HHS) for investigation or compliance review; or
    e. Other uses and disclosures that are permitted or required by law, for example, mandatory reports of abuse and neglect, uses and disclosures for governmental health oversight activities, and disclosures for judicial and administrative proceeding and pursuant to a lawful subpoena or court order.

2. **Safeguarding Paper and other Tangible PHI**

    a. Do not remove tangible PHI from a business or clinical unit unless approved by the Compliance Director;
    b. If allowed to remove PHI, do not leave it, or any file, box, briefcase or portable electronic device containing PHI anywhere they can easily be stolen such as in a car;
    c. Avoid displaying or storing PHI in public spaces or in spaces that visitors must pass through;
    d. Do not leave PHI on desks when not working on it. Safely store PHI even if you step away from your desk or work area for a minute;
    e. Lock PHI away in a file cabinet or locked office at the end of the day;
    f. Always dispose of PHI in secure shredding bins.
    g. If mailing PHI, you can use U.S. Mail or other delivery services like UPS or FedEx, but secure PHI appropriately by using an inner envelope sealed, addressed and marked "confidential" before placing it in the outer envelope or mailing box. Don't overstuff to avoid damage in transit.
    h. If mailing electronic media, such media must be encrypted unless a patient requests information on electronic media and requests that it not be encrypted.
    i. If sending PHI via FAX, confirm the recipient and the FAX number, use a coversheet that provides a disclaimer and your contact information in the event of an error, then confirm receipt. Never put PHI on the coversheet.

3. **Safeguarding Verbal PHI**

    a. **Conversations**. Do not discuss patient information in public areas or with any person who does not have a need to know the information.
    b. **Waiting Rooms or Customer Service Areas.** Waiting rooms and customer service areas are not considered clinical areas. Staff should be careful not to disclose clinical information in these areas and will restrict conversations to the minimum necessary information.

c. **Landlines and Mobile Phones.** Use commonsense precautions such as ensuring no one is in the vicinity when making a call. Avoid use of speakerphones. When leaving a voicemail, leave the minimum necessary information unless the patient or his/her personal representative has authorized you to leave detailed messages.

4. Safeguarding Electronic PHI (ePHI)

a. Only use electronic devices that are approved for use.
b. Only store ePHI on approved electronic devices with encryption.
c. When sending ePHI via email: Ensure the recipient is authorized access to the ePHI and use encryption. Do not put PHI in the subject line of the email.
d. If a patient requests use of non-secure email, explain the risks to the patient and document the request. Limit information to the minimum necessary if possible. Encourage us of a secure patient portal.
e. Do not send PHI via text messages unless you use an approved and secure texting application.
f. Do not position monitors displaying ePHI where they can be viewed by the public. If they cannot be repositioned, install privacy screens.
g. Protect accounts, passwords and workstations:

    i. Create and periodically change passwords. A password with a mix of at least 12 characters and numerals is a best practice.
    ii. Immediately change your password and notify Information Security if you believe your password has been disclosed, accessed or used by an unauthorized person.
    iii. Do not share your passwords with any other person.
    iv. Do not use CHLAMG passwords for non-CHLAMG accounts.
    v. Only use administrator accounts with privileges as authorized and necessary.

h. Only use encrypted removable media (USB drives) for storing ePHI.
i. Avoid duplicative storage of ePHI on devices by securely deleting or removing unnecessary electronic copies.
j. Report to the Compliance Director or the CHLA Chief Information Security Officer (CISO) any unusual system activity including:

    i. Alerts displayed by a system or application indicating a problem;
    ii. Unusual behavior such as loss of control of a mouse or keyboard;
    iii. Alerts displayed by security software meant to prevent malicious code.

k. Report to the Compliance Director or the CHLA CISO potential security events such as:

    i. The loss of any device (personal or CHLA/CHLAMG-owned) containing PHI;
    ii. Unusual account activity such as last login occurring at an unusual time; or
    iii. Someone accessing PHI who is not authorized to do so.

l. Dispose of PHI which means files on computer systems must be securely deleted and media must be physically destroyed when no longer needed. Hard drives are wiped and placed in secured storage until they are shredded.
m. Copiers/printers connected to CHLAMG information systems are protected by firewalls and other security features to protect against intrusion.
n. Photos, audio recordings and video recordings have the same safeguards as other ePHI.

5. Questions regarding interpretations of this policy should be directed to CHLAMG Compliance at 323.361.2173 or by email to CHLAMGCompliance@chlamg.usc.edu.

REFERENCES:

45 CFR 164.506
Confidentiality of Medical Information Act, Cal. Civ. Code Sections 56-56.16

POLICY OWNER: CHLAMG Compliance Director

Approved by CHLAMG Executive Compliance Committee on December 26, 2018.