Children's Hospital LOS ANGELES Medical Group	**POLICY AND PROCEDURES**		
	POLICY NUMBER:	CHLAMG-CI-1013	
	ORIGINAL DATE: 11/1/2018	REVISED:	EFFECTIVE: 12/26/2018
DEPARTMENT: Compliance	APPROVED BY: Carl Grushkin, MD and Chief Compliance Officer		
POLICY TITLE: **Facility Access Control**			

PURPOSE:

Children's Hospital Los Angeles Medical Group (CHLAMG) is committed to conducting organizational business in compliance with all applicable laws, regulations, and CHLAMG policies. CHLAMG has adopted this policy to ensure that physical access to confidential data is appropriately limited. The scope of this policy covers the process that limits physical access to electronic information systems and the facility or facilities in which such systems are housed, while still ensuring that proper authorized access is allowed.

DEFINITIONS:

Confidential Data/confidential information for the purposes of this policy shall be any information, regardless of format, about patients, workforce members, students, residents, providers or business operations that should not be made available to the public without specific authorization. Loss or inappropriate access to this information could harm patients and impair CHLAMG's ability to do business. Confidential information includes, but is not limited to, Protected Health Information (PHI), electronic PHI, Personally Identifiable Information (PII) including Social Security Numbers, cardholder data (PCI), and financial information. Examples of confidential information include: personnel records, privileged information from legal counsel, any board, board committee minutes, notes or actions, non-public financial, strategic or operational information, and any other information deemed confidential by CHLAMG.

SCOPE: This policy covers requirements for those assets and areas that are not managed by CHLA information services.

POLICY:

A. **WORKSTATION SECURITY.** PMG Information Services is responsible for implementing physical and technical safeguards to ensure the confidentiality, integrity, and availability of information, including Confidential Data, for all workstations, and to restrict access to authorized users.

1. Users are required to receive education on the appropriate use of technology and are required to abide by all applicable policies.
2. Users are prohibited from downloading applications, removing applications, or altering their workstations in any manner other than that configured by CHLAMG Information Services.
3. Users must follow password and computer setting policies.
4. Users are responsible to appropriately store and transmit data, including Confidential Data, in accordance with relevant policies
5. Users must exercise reasonable care to physically protect their devices by:
    a. Preventing accidental spills by keeping food and drink away from workstations
    b. Ensuring workstations are logged off or shut down when not in use.
    c. Ensure all workstations use a surge protector or a UPS battery back-up.
6. Devices that transmit PHI are required to be encrypted.
7. Users who separate or terminate from the organization must:
    a. Return all electronic communication devices on or before the last day as an authorized user;
    b. Not delete or erase any emails, attachments or files;

c. Not copy data to a portable cloud or storage;
d. Not send any emails, with or without attachments, internally or to their personal or other external email accounts such as Gmail and Yahoo; and
e. Not print and depart with any emails, attachments or files. Such action may be considered theft of CHLAMG/PMG intellectual property and could result in legal action.

B. **FACILITY SECURITY PLAN.** PMG occupies leased space at 3701 Wilshire Blvd., Suite 600, Los Angeles and at 800 N. Brand Blvd, 11th Floor, Glendale. The Facility Security Plan includes the following components:

1. Contingency Operations – procedures that allow physical facility access during emergencies to support restoration of data under a Disaster Recovery Plan. (See CHLA MIS 15.0 Data Backups and Contingency Planning.)
2. Access Control and Validation. PMG staff are issued photo ID badges and all entrances to the suite require badge access 24/7 except for main entry to the reception area. The main entry requires badge access between the hours of 1630 – 0730. The reception area is manned during the hours of 0730 – 1630. Appropriate credentials or escort is required beyond the reception area. All visitors are required to sign-in.
3. Physical Access Records–Server Room Security. The PMG Server Room is secured at all times and is accessible by PMG Information Services Staff with badge access. If the lessor requires access to this space for repair/maintenance, the lessor's staff is escorted and accompanied until work is completed.
4. Maintenance Records. Procedures to document and manage repairs and modifications to the physical security components of the facility including locks, doors, and other physical access control hardware. The Office Administrator maintains an inventory and controls for all keys and access cards and the individuals they are assigned to.
5. Staff are issued keys to securely lock confidential data in paper form in desks and filing cabinets.
6. Shredding bins are provided for the secure disposal of discarded paper PHI.
7. Locations are equipped with smoke detectors and with accessible fire extinguishers. Risk of water damage is minimized by location on upper floors.

C. WORKFORCE ACCESS CONTROLS

1. CHLAMG establishes and implements appropriate procedures to control and validate workforce member access to all facilities used to house CHLA data and systems.
2. CHLAMG ensures that its workforce members wear their Identification Badges when performing duties.
3. CHLAMG workforce badges are to be deactivated upon termination, voluntary or non-voluntary.
4. CHLAMG workforce members are authorized and encouraged to challenge unrecognized personnel.

D. VISITOR ACCESS CONTROLS

1. CHLAMG establishes and implements procedures to control, validate, and document visitor access to any facility used to house CHLA data and systems. Visitors include vendors, repair personnel, and other non-CHLAMG personnel.
2. All visitors who require access to facilities containing CHLAMG data and systems sign in and provide information regarding their identity and the purpose of their visit.
3. All visitors are to be escorted to and from their destination and are with CHLAMG personnel at all times.

E. NON-COMPLIANCE

1. Non-compliance with this policy will be regarded as a serious matter because these actions may compromise the confidential, security and integrity of CHLAMG facilities and its confidential information. Appropriate corrective action will be taken when a violation is identified. Any failure to abide by this policy may result in disciplinary action including revoking or restricting any right to system access, and may lead to more serious disciplinary action in accordance with CHLAMG disciplinary policies up to and including termination of employment and individual legal liability.

POLICY OWNER: CHLAMG Compliance Director

Approved by CHLAMG Executive Compliance Committee on December 26, 2018