LOS ANGELES GENERAL MEDICAL CENTER POLICY

Subject:	Original Issue Date:	Policy #
PRIVACY COMPLIANCE PROGRAM	4/14/03	**120**
	Supersedes: 2/7/17	Effective Date: 11/6//23

Policy Owner(s): Director, Health Information Management
Executive Sponsor(s): Chief Operations Officer

Departments Consulted:	Reviewed & approved by:	Approved by:
Office of Human Resources Information Systems Health Information Management	Attending Staff Association Executive Committee Senior Executive Officer	Chief Operations Officer Chief Executive Officer

PURPOSE

To define the Privacy Compliance Program for the Los Angeles General Medical Center.

POLICY

The administrative requirements for the Medical Center's Privacy Program consist of twelve sections:

I. Privacy and Confidentiality Training
II. Disciplinary Actions for Failure to Comply with Privacy Policies and Procedures
III. Safeguards for Protected Health Information
IV. Disclosure of Protected Health Information (PHI) by Whistleblowers
V. Workforce Member Crime Victims
VI. Mitigation
VII. Non-Retaliation
VIII. Waiver of Rights
IX. Complaints Related to Los Angeles General Medical Center Privacy Practices
X. Privacy Office Designations
XI. Implementing Changes to Privacy-Related Policies
XII. Documentation of Privacy Policies and Procedures

Privacy and Confidentiality Training

To ensure that members of the Medical Center workforce understand their role and responsibility in protecting patient privacy, the Medical Center provides privacy and confidentiality training to all workforce members. In addition to new hire and annual training, training is an intricate part of the facilities' corrective action in response to a privacy breach. Occurrence of training includes:

1. An initial training of all current Medical Center workforce members at or near the time the privacy regulation becomes effective.

2. Training of new workforce members occurs within a reasonable time period (30 calendar days) following the member's addition to the workforce.

3. Retraining of workforce members whose job duties are affected by a material change in policy and/or procedure.

4. In the event of a privacy breach investigation, a tailor HIPAA training is provided to meet the employee or department's need to access protected information to perform assigned duties or functions.

Training will be documented and maintained in either electronic or written format for each workforce member for six years.

Disciplinary Actions for Failure to Comply with Privacy Policies and Procedures

A. The Medical Center has policies and procedures regarding discipline that are communicated to all workforce members, agents, and contractors. Examples of possible sanctions or discipline include, but are not limited to, verbal warnings, notices of disciplinary action placed in personnel files, removal of system privileges, termination of employment, and sanctions or penalties imposed pursuant to contract. Workforce members, agents, and contractors are also advised that there may be civil or criminal penalties for misuse or misappropriation of protected health information (PHI) and violations may result in notification to law enforcement, regulatory, accreditation, and licensure organizations.

B. If there is reason to believe a member of the workforce has failed to follow the privacy policies, security protocols, or breached patient confidentiality, then an investigation will be initiated and documented. If the allegation is substantiated through the investigation, appropriate sanctions or discipline will be applied.

C. The Medical Center will maintain documentation related to sanctions of its workforce in either electronic or written format. This documentation will be retained in the workforce member's personnel record or other appropriate location depending on the category of the workforce member involved. This process will be imposed equitably throughout the Medical Center. Sanctions or discipline will be applied commensurate with the severity, frequency, and intent of the violation or breach.

Safeguards for Protected Health Information

Safeguards are the administrative, technical, and physical protective measures and controls the Medical Center imposes to protect the privacy of PHI from intentional or unintentional disclosure. These safeguards include but are not limited to: hardware and software security features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas, and devices.

A. The Medical Center develops and maintains policies, procedures, and technical processes that assure appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.

B. These safeguards provide reasonable protection of PHI from intentional or unintentional use or disclosure.

C. The Medical Center is responsible for creating, implementing, and maintaining a risk management plan for both electronic and non-electronic information assets.

D. Verification of the development of safeguards is a responsibility of the Medical Center Privacy Office who will consult with, Department of Health Services (DHS) Privacy Office, Security Coordinators, and/or other knowledgeable individuals.

Disclosures of Protected Health Information by Whistleblowers

The Medical Center does not violate the privacy regulations if a member of the Medical Center workforce discloses PHI to a health oversight agency, public health authority authorized to investigate, health care accreditation organization, or to an attorney retained by a workforce member if the purpose of the disclosure is to report an allegation of unlawful conduct by the Medical Center, a violation of professional or clinical standards, or conditions that endanger patients.

Workforce Member Crime Victims

The Medical Center does not violate the privacy regulations if a member of its workforce, who is a victim of a crime, discloses PHI about the suspected perpetrator to a law enforcement official and the information disclosed is limited to the following information:

- Name and address,
- Date and place of birth,
- Social security number,
- ABO blood type and RH factor,
- Type of injury,
- Date/time of treatment,
- Date/time of death (if applicable), and
- Distinguishing physical characteristics (e.g., weight, height, gender, race, hair/eye color, facial hair, scars/tattoos).

Mitigation

To the extent practicable, the Medical Center will mitigate any known harmful effects from the use or disclosure of PHI that was in violation of Medical Center security or privacy policies and procedures.

Non-Retaliation

The Medical Center will not intimidate, threaten, coerce, or retaliate against persons for filing complaints; for testifying, assisting, or participating in investigations; assisting or participating in compliance reviews; assisting or participating in proceedings or hearings under Part C of Title XI of the Social Security Act; or for opposing real or perceived unlawful acts or practices under this act provided the opposition is reasonable.

Waiver of Rights

The Medical Center does not require an individual to waive his or her right to file a complaint or other rights with regard to his or her respective PHI as a condition for the provision of treatment, payment, or employment.

Complaints Related to the Los Angeles General Medical Center Privacy Practices

A. The Medical Center provides a process for filing a complaint or grievance regarding privacy practices.

B. All complaints or grievances are investigated and documented. This documentation includes outlining the facts of the complaint or grievance, the investigative procedures and outcomes, and final resolution. The Medical Center maintains in either electronic or written format, documentation related to the filing of a complaint by an individual. This documentation will be retained for six years from the date of its creation or the date when it last was in effect, whichever is later.

Privacy Office Designations

A. The Medical Center has designated a Privacy Officer who is responsible for the development and implementation of the policies and procedures of the entity.

B. The Medical Center has designated Privacy Compliance Office that is responsible for receiving complaints and is able to provide further information about matters covered by the Joint Notice of Privacy Practices.

Implementing Changes to Privacy-Related Policies

Medical Center's policies and procedures concerning PHI are implemented, revised, or changed as necessary or required due to changes in the law, health care practice, or entity situation. Policy or procedures that do not materially affect the content of the Joint Notice of Privacy Practices are not changed unless the policy or procedural revisions are necessary to comply with the privacy regulations or the policy or procedure is documented prior to the effective date of the change.

A. Necessary revisions or changes in policies, procedures, or the Joint Notice of Privacy Practices (Notice) are documented and implemented in a timely manner. When applicable, affected groups receive notification of the changes.

    1. Policy and procedural implementation relative to a Notice are not made prior to the effective date of the Notice.

    2. The Medical Center reserves the right to make changes to the Notice needed to comply with revised federal and/or State privacy regulations or changes in DHS's privacy policies.

3. Changes of this type relate only to PHI received or created after the effective date of the Notice and are implemented after that effective date.

Documentation of Privacy Policies and Procedures

The Medical Center documents and maintains in a written or electronic format all policies, procedures, and communications relating to the privacy practices for six years from the date of creation or the last date it was in effect, whichever is the longest.

The Medical Center administrative department heads/managers, physician department chairs or unit medical directors, and others as appropriate are responsible for the development, potential review and revision of the policies and procedures, and communications for their respective area(s). The period between reviews will not exceed three years.

All privacy related policies and procedures that affect the Medical Center should be approved in accordance with the Medical Center's policy and procedure approval process.

REFERENCES

45 Code of Federal Regulations, Part 160 and 164; Section 164.530 "Administrative Requirements" and Section 164.502 "General Rules"
TJC **RI.01.01.01.07 , RI.01.01.01.10 , RI.01.01.01.37**
CMS 482.13 (c), (d)
DHS Policy No. 361.1, Department of Health Services' Privacy Compliance Program
DHS Policy No. 361.2, Notice of Privacy Practices
DHS Policy No. 361.10, Disciplinary Actions for Failure to Comply with Privacy Policies and Procedures
DHS Policy No. 361.11, Complaints Related to the Privacy of Protected Health Information (PHI)
DHS Policy No. 361.12, Waiver of Rights
DHS Policy No. 361.13, Non-Retaliation
DHS Policy No. 361.22, Implementing Changes to Privacy-Related Policies
DHS Policy No. 361.23, Safeguards for Protected Health Information
DHS Policy No. 361.24, Privacy and Confidentiality Training
DHS Policy No. 361.26, Mitigation

REVISION DATES

April 10, 2007; September 25, 2008; November 12, 2013; February 7, 2017; November 6, 2023