

# LOS ANGELES GENERAL MEDICAL CENTER POLICY

Subject: <b>HEALTH/MEDICAL RECORD: ELECTRONIC SIGNATURES</b>		Original Issue Date: 4/19/05	Policy # <b>413</b>
		Supersedes: 10/10/17	Effective Date: 8/8/23
Policy Owner(s): Director of Health Information Management Executive Sponsor(s): Chief Operations Officer			
Departments Consulted: Health Information Management Information Systems Nursing Services Medical Administration Health Information Committee	Reviewed & approved by: Attending Staff Association Executive Committee Senior Executive Officer	Approved by:  Chief Operations Officer	
		Chief Executive Officer	

## PURPOSE

To describe the Los Angeles General Medical Center standards for electronic signatures as applied to electronic health/medical record documentation.

To ensure that authentication of electronic documents complies with applicable federal and State laws and regulations, Los Angeles County Department of Health Services policies, and accreditation standards.

## POLICY

To qualify as an electronic signature, any proposed scheme must use an additional piece of information (e.g., hosted password), or other Biometrics identification device, to complete the authentication process. Re-entry of the password at the time of signing is an acceptable alternative for systems. Saving the document authenticates the user and is validation of entry within the electronic record. Name, credentials, date and time are stamped on the electronic record.

Providers, who use computers to sign electronic documents, must sign a statement assuring that they alone will use their access to the electronic medical record system.

Electronic signatures will comply with the following standards:

- Data integrity to protect information from accidental or unauthorized change (for example "locking" of the entry so that once signed no further changes can be made to the entry);
- Authentication to validate the correctness of the information and confirm the identity of the signer (for example requiring signer to authenticate with password or other mechanism);
- Non-repudiation to prevent the signer from denying that he or she signed the document (e.g., unique identifiers to support authenticity of hosted password for access to the EMR);

		Page 2	Of 2
Subject: <b>HEALTH/MEDICAL RECORD: ELECTRONIC SIGNATURES</b>	Effective Date: 8/8/23	Policy # <b>413</b>	
	Chief Executive Officer's Initials:		

- At a minimum, the electronic signature must include the full name and credentials of the author, and date and time (including time zone) signed.

Countersignatures or dual signatures must also comply with the authentication requirements.

**RESPONSIBILITY**

Administration  
 Attending Staff  
 Residents  
 Allied Health Professionals  
 Nursing Staff  
 Health Information Management  
 Information Systems

**PROCEDURE DOCUMENTATION**

Health Information Management Policy and Procedure Manual

**REFERENCES**

California Code of Regulations, Title 22, Sections 70749, 70223(f-h)  
 Joint Commission Standards RC.01.02.01  
 CMS 482.24 (c)

**REVISION DATES**

October 03, 2008; July 10, 2012; November 12, 2013; October 10, 2017; August 8, 2023