EMR Documentation Guidelines

EMR ELEMENT	GUIDELINE
Authenticity, Integrity, and Confidentiality	Passwords must not be shared[4]. No one can chart in a record opened up under someone else's password[5]. Violations will be reviewed on a case-by-case basis by the Chief Compliance Officer and may result in disciplinary action[5].
Authorship Integrity	Each entry in the patient record must be time and date stamped by the author[1].
Documentation Integrity	Documentation must be specific to a patient's condition at the time of his/her encounter and must accurately represent the service(s) rendered. EMR documentation that is identical among records is considered a misrepresentation of the medical necessity requirement for coverage of services. Templates should be based on clinically appropriate, standards-based protocol for common or routine information. Documentation must reflect an active choice in response to the interaction with the patient[3]. Pre-populated outcomes are not permitted in the use of templates. Copying previously entered text may enhance documentation efficiency; however improper use of documentation tools compromises the integrity and quality of the medical record. Appropriate modification and editing are essential to ensure documentation reflects the history, exam, assessment, and plans of the physician for each specific encounter[3]. • Documentation elements that must never be copied include the History of Present Illness, Exam, and Assessment & Plan. • Only judicious copying of an author's own content is acceptable.
Documentation Timeliness	Documentation should be generated at the time of service or within a reasonable timeframe shortly thereafter.
Data Integrity	All diagnoses pertinent to the current episode of patient care should be documented to the highest degree of specificity[2].

SOURCE INFORMATION:

1. 'Guidelines for Teaching Physicians, Interns, and Residents,' Centers for Medicare & Medicaid Services (CMS)
2. 'Evaluation & Management Services Guide,' Centers for Medicare & Medicaid Services (CMS)
3. 'Maintaining a Legally Sound Health Record – Paper and Electronic,' American Health Information Management Association (AHIMA)
4. Health Information Portability and Accountability Act (HIPAA) Administrative Simplification Regulations, Sub Part C – Security Standards for the Protection of Electronic Protected Health Information, http://www.hhs.gov/ocr/hipaa/finalreg.html
5. Password Security Policy, Northwestern Medical Faculty Foundation, Approved March 2002