

Module IV - Table of Contents – In Detail

Chapter 17. Two-Fold Legality

Two-Fold Legal Aspects of Medical Documentation	380
---	-----

Chapter 18. Legal Regulations

The HIPAA Privacy Rule of 2003	383
--------------------------------------	-----

Legal Aspects of Regulatory Compliance	383
--	-----

SuperScribe Tip:	385
------------------------	-----

The HIPAA Security Rule of 2005	386
---------------------------------------	-----

SuperScribe Tip: Covered Entity and Business Associate	386
--	-----

Administrative Safeguards	387
---------------------------------	-----

SuperScribe Tip: Your ePHI Access is Specialized to your Authorization Credentials	389
--	-----

Physical Safeguards	390
---------------------------	-----

Technical Safeguards	391
----------------------------	-----

Organizational Requirements	393
-----------------------------------	-----

The Health Information Technology for Economic and Clinical Health Act (HITECH)	393
---	-----

HIPAA and HITECH Final Enforcement Rules & Breach Notification Rules	394
--	-----

CMS Requirements for Medical Documentation	395
--	-----

SuperScribe Tip:	395
------------------------	-----

CMS' Legal Requirements for Hospital Medical Record Services and Content	396
--	-----

CMS' Legal Requirements for Clinical Record Content for specialized providers	399
---	-----

Review & Assessment	401
---------------------------	-----

Recommended Resources	401
-----------------------------	-----

Review	401
--------------	-----

Assessment	405
------------------	-----

Chapter 19. The Legal Medical Record

Patient Care Documentation	407
----------------------------------	-----

Clinical-, Business-, and Legal Health Record Documentation	407
---	-----

Public Health Documentation	408
-----------------------------------	-----

SuperScribe Application: The Clinical Medical Record (CMR)	408
--	-----

Financial Documentation	409
Legal Documentation	411
The Legal Business Record and The Legal Health Record (LHR)	411
SuperScribe Tip:	411
The Business Record	412
The Legal Health Record.....	412
Review & Assessment.....	414
Recommended Resources.....	414
Review	415
Assessment.....	417
 Chapter 20. Medicolegal Documentation	
Chapter 21. (I): Audits & Amendments	
Legal Health Record Documentation	419
Audit Trails and Electronic Record Discovery	420
Documentation Amendments.....	422
Review & Assessment.....	425
Review	425
Assessment.....	426
 Chapter 22. Medicolegal Documentation	
Chapter 23. (II): The Expanded SOOOAAP Note	
The Expanded SOOOAAP Note Format for Medico-Legal Documentation.....	428
SuperScribe Tip:	432
Review & Assessment.....	433
Recommended Resources.....	433
Review	433
Assessment.....	434
 Chapter 24. Malpractice Prevention	
Fraud and False Claims Acts.....	436

Reducing Legal Risk in Documentation.....	438
SuperScribe Tip#1: “If It Was Not Documented, It Did Not Occur”	438
SuperScribe Tip #2: Document with Accuracy – Check and Re-Check!	440
SuperScribe Tip #3: Document Medically Necessary Information	442
SuperScribe Tip #4: Document Objectively.....	443
SuperScribe Tip #5: Document Precisely.....	444
SuperScribe Tip #6: Document with Grammatical Accuracy	445
SuperScribe Tip #7: Document Timing in a Timely Manner.....	446
SuperScribe Tip #8: Document Consistently.....	446
Review & Assessment.....	447
Recommended Resources.....	447
Review	447
Assessment.....	449
References:.....	450

A close-up photograph of a medical report form titled "MEDICAL REPORT" from the "State of New Mexico". A silver stethoscope is placed on the left side of the form, and a wooden gavel with a brass head is on the right. The form contains text about medical examinations for motor vehicle drivers, including a section for "PLEASE TYPE OR PRINT" and fields for "First, Middle Initial)", "Social Security Number", and "Driver License Number".

17

Two-Fold Legality

Two-Fold Legal Aspects of Medical Documentation

Chapter 1 of this manual identifies the **4 Pillars of Medical Documentation**, which include:

- General Aspects
- Medical Aspects
- Financial Aspects
- Legal Aspects

The legal aspects of medical documentation that pertain to clinical scribes are two-fold, involving:

- **Legal Regulations:**
 - ▶ Legal obligations to comply with HIPAA & HITECH Standards
 - ▶ Legal obligations to comply with other standards that protect against fraudulent coding, billing, and reimbursement claims for medical services (such as E/M Service Documentation)
- **The Medical Record as a Legal Document:**
 - ▶ Legal Medical Record (LMR), as distinct from the Clinical Medical Record (CMR)

These two legal aspects of the clinical scribe role are often intertwined. However, we have separated them in this module, with both aspect addressed individually in chapters 18 and 19. No doubt you have already noticed that some of the important legal aspects of medical documentation have already been introduced in this manual. Before commencing with the rest of this module, we suggest you review the following sections of this manual to solidify your introduction to the legal aspects of medical documentation:

Module I: General & Regulatory Aspects of Medical Documentation

- Chapter 5: Industry Regulation (HIPAA & HITECH)

Module III: Financial Aspects of Medical Documentation

- Chapter 12: Historical Overview of the Healthcare Industry
- Chapter 13: MACRA & QPP
- Chapter 15: E/M Coding in Depth

Once you have reviewed the above chapters, we invite you to commence with this module!

- **Chapter 18 – Legal Regulations:**
 - ▶ Important aspects of HIPAA & HITECH policy are reviewed
- **Chapter 19 – The Legal Medical Record (LMR):**
 - ▶ The Legal Medical Record (LMR) is introduced and distinguished from the clinical medical record (CMR), and from the Designated Record Set (DRS)
- **Chapter 20 – Medicolegal Documentation I:**
 - ▶ Audit Logs
 - ▶ Documentation Amendments
- **Chapter 21 – Medicolegal Documentation II:**
 - ▶ SOOOAAP note documentation is reviewed as the medicolegal documentation standard for preventing malpractice
- **Chapter 22 – Malpractice Prevention Tips:**
 - ▶ Best Practices in Medical Documentation are provided in light of a variety of literature on medical malpractice documentation claims



18

Legal Regulations

Legal Aspects of Regulatory Compliance

Medical records can be used in court as evidence. Therefore, all medical documentation of- and interaction with patient health information have potential to constitute access to legal evidence, and should be conducted accordingly. Creating, accessing, altering, and/or deleting medical health records or patient health information has the potential to constitute

tampering with- and/or destroying legal evidence, and should be viewed as such by all clinical scribes. In order to protect the legal authentication of a medical record, it is important to ensure that all interactions with medical health records and patient health information comply with organizational-, state-, and federal policies.

Module I of this manual introduces regulations, policies, and procedures regarding the role of the Clinical Scribe. Some of the regulations have legal implications, as addressed in Chapter 5, which introduces the **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** and the **Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009**. Here, we will review several aspects of these Federal Regulations as they pertain *legally* to the Clinical Scribe role and to the way in which patient health information (including medical health records) may be accessed in order to preserve the legal authenticity of medical documentation. These issues are covered in greater detail in Appendix A.VIII.

The HIPAA Privacy Rule of 2003

HIPAA's Privacy Rule is addressed in Chapter 5 of Module I and provides a set of standards regarding the use and disclosure of **protected health information (PHI)**^{10,11}. Three concepts that are central to the Privacy Rule include those of individually identifiable health information, protected health information (PHI), and the “Minimum Necessary” use of PHI, as addressed below.

- **Health Information:**
 - ▶ *“Any information ... whether oral or recorded in any form or medium that: (1) is created or received by a health care provider [or other health care organization or entity]; and (2) relates to the past, present, or future physical or mental health or 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 individual².”*

- **Individually Identifiable Health Information:**
 - ▶ A subset of health information that includes “*demographic information collected from an individual, and: ... (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual².*”
- **Protected Health Information (PHI):**
 - ▶ “Individually identifiable health information ... that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium².” Exclusions include: “(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer².”
- **“Minimum Necessary” Rule:**
 - ▶ This principle is central to HIPAA’s Privacy and Security rules and provides the official policy regarding the use and disclosure of PHI and ePHI. Title 45 of the Code of Federal Regulations (CFR) § 164.502(b) states: “*Minimum necessary applies when using or disclosing PHI or when requesting PHI from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request¹⁵.*”

The Privacy Rule also addresses **Administrative Requirements** which are outlined in Chapter 5. In general, the Privacy Rule requires each covered entity to develop and implement^{10,11}:

- **Written Privacy Policies and Procedures** that are consistent with the Privacy Rule
- **Privacy Personnel** including a designated privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or office responsible for receiving complaints and providing individuals with information on the covered entity’s privacy practices.
- **Training, Management, and Enforcement** of privacy policies and procedures for all workforce personnel – including employees, volunteers, and trainees – which includes appropriation of sanctions against workforce members who violate the entity’s privacy policies and procedures or the Privacy Rule.

- **Data Safeguards** to maintain “reasonable and appropriate administrative, technical, and physical safeguards [that] prevent intentional or unintentional use or disclosure of PHI in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure¹⁰.”
 - ▶ These safeguards are addressed in Chapter 5 and include **Login Authorization**, such as individually identifiable username and passwords for each individual personnel.



SuperScribe Tip:

Independent Clinical Scribes are legally responsible for their own HIPAA Privacy Rule Compliance. Your Healthcare Provider or Organization is legally required to provide you with the following Privacy Rule Requirements (as described above):

- **Written Privacy Policies and Procedures**
- Access to **Privacy Personnel**
- **Training, Management, and Enforcement on- and of its privacy policies and HIPAA Compliance**
- **Data Safeguards**, such as individual login authorization and information

As an independent clinical scribe, you are also responsible for HIPAA compliance. We encourage you to ensure that you have access to:

- Your healthcare organization’s written privacy policies and procedures
- Contact information for your organization’s privacy personnel
- Your organization’s training procedures and policies regarding privacy management and enforcement.
 - ▶ You must receive HIPAA training from your healthcare organization
 - ▶ You will be held subject to your healthcare organization’s privacy management and enforcement policies
- Your healthcare organization’s data safeguards, including information on individually identifiable authorization and access to your facility’s electronic health record system.

As an Independent Clinical Scribe, you are legally responsible for compliance with HIPAA’s Privacy Rule



SuperScribe Tip: Covered Entity and Business Associate

The terms “Covered Entity” and “Business Associate” are defined as follows:

- Covered Entity: refers to “any health care provider, health plan, or health care clearinghouse that transmits any health information in electronic form in connection with a HIPAA transaction².”
- Business Associate: refers to “a person who: on behalf of a covered entity or an organized health care arrangement... in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs or assists in the performance of:
 - ▶ (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
 - ▶ (B) Any other function or activity regulated by this subchapter...²”

The HIPAA Security Rule of 2005

Whereas the HIPAA Privacy Rule pertains to all PHI (including paper and electronic), the HIPAA **Security Rule** pertains specifically to **electronic protected health information (ePHI)**, which is defined as follows:

- **Electronic Protected Health Information (ePHI):** Individually identifiable health information that is transmitted by- or maintained in **electronic media**, which includes:
 - ▶ “(1) *Electronic storage media [such as] memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or*
 - ▶ (2) *Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media.*

- ▶ *Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission².*

The HIPAA Security Rule provides a set of **Security Standards** that govern the use and disclosure of ePHI. Several important Security Standards are identified and defined below¹⁶⁻¹⁸:

- **Administrative Safeguards:** *“Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information¹⁶.”*
- **Physical Safeguards:** *“Physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion¹⁷.”*
- **Technical Safeguards:** *“The technology and the policy and procedures for its use that protect electronic protected health information and control access to it¹⁸.”*
- **Organizational Requirements:**
 - ▶ Include security standards and requirements for **business associate contracts** or other arrangements and group health plans¹⁹.
 - ▶ Provides a standard set of **general rules for security policies and procedures**, which take a “flexibility approach” similar to that outlined for HIPAA’s privacy policies and procedures (identified above and described below)¹⁹.
 - ▶ Provides **documentation standards** that relate specifically to documentation time limits, availability, and updates¹⁹.

Chapter 5 (Module I) highlights some of the Security Standards that apply to the role of the clinical scribe. Here, we will provide some additional information on these standards as they pertain to the scribe role *from a legal perspective*.

Administrative Safeguards

HIPAA’s Security Rule sets the following **Administrative Safeguard Standards**, which legally apply to all Clinical Scribes:

- **Security Management Process(es):** This standard requires covered entities to *“implement policies and procedures to prevent, detect, contain and correct security violations¹⁶.”* This

standard includes two specific implementation requirements that apply legally to the medical scribe role:

- ▶ The **Sanction Policy** requires covered entities to “*apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity*”¹⁶.
- ▶ Covered entities are also required to implement **Information System Activity Reviews(s)**, which must include “*procedures to regularly review records of information system activity, such as **audit logs, access reports, and security incident tracking reports***”¹⁶.

Information Security Activity Reviews Monitor All Scribe Activity within the EHR

As healthcare employees with authorized access to ePHI:

- Each of your EHR system logins will be recorded and subject to auditory review.
- All ePHI that you access within your facility’s EHR system will be recorded and subject to auditory review.
- All EHR entries that you create, access, change, or delete will be recorded and subject to auditory review.

Any activity found to be in violation of the HIPAA Security Rule and/or the covered entity’s security policies is subject to the sanction and enforcement policies of the covered entity and those set forth in the HIPAA Enforcement Rule (below).

- **Workforce Security:** This standard requires covered entities to “*implement policies and procedures to ensure that all members of its workforce have appropriate access to ePHI ... and to prevent those workforce members who do not have access ...from obtaining access to ePHI*”¹⁶. This standard includes two specific implementation requirements that apply legally to the medical scribe role:
 - ▶ Covered entities are required to implement procedures to “[**authorize and/or supervise**] workforce members who work with ePHI or in locations where it might be accessed”¹⁶.
 - ▶ Covered entities are also required to “*implement **procedures for terminating access to ePHI** when the employment of a workforce member [including a clinical scribe] ends or as required by determinations made as specified in [the Workforce Clearance Procedure]*”¹⁶.

- **Information Access Management:** This standard requires covered entities to “*implement policies and procedures for authorizing access to ePHI that are consistent with [the Privacy Rule]¹⁶.*” This standard includes two specific implementation requirements that apply legally to the medical scribe role:
 - ▶ **Access Authorization:** HIPAA’s Workforce Security Standard requires covered entities to determine “*whether a particular user [such as a clinical scribe] ... has the right, based on job function or responsibilities, to carry out a certain activity, such as reading a file or running a program¹⁶.*” The entity is also required to “*implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.*”
 - ▶ **Access Establishment and Modification:** This specification requires covered entities to “*implement policies and procedures that, based upon the entity’s access authorization policies, establish, document, review, and modify a user’s right of access to a workstation, transaction, program, or process¹⁶.*”



SuperScribe Tip: Your ePHI Access is Specialized to your Authorization Credentials

The Information Access Management Security Standard requires covered entities – including the healthcare organization that you work for- or with in your role as a clinical scribe – to provide you with the minimum necessary access authorization to ePHI. For this reason, it is critical that you and only you use your authorized credentials (such as login username and password) to access ePHI during your role as a clinical scribe.

- In your role as a clinical scribe, you may not use ePHI access (such as login information) authorized to other individuals, or authorized to you in another clinical role (such as that of an MA or NPP). You may not allow other individuals to use your access credentials.
- **Security Awareness and Training:** This standard requires covered entities to “*implement a security awareness and training program for all members of its working¹⁶.*” This standard includes two specific implementation requirements that apply legally to the medical scribe role:
 - ▶ Covered entities must implement policies and procedures for “*guarding against, detecting, and reporting **malicious software**¹⁶.*”

- ▶ **Log-in Monitoring and Password Management:** As identified in Chapter 5, your healthcare facility is responsible for implementing “*procedures for monitoring log-in attempts and reporting discrepancies*” and for “*creating, changing, and safeguarding passwords*”¹⁶.
- **Security Incident Procedures:** This standard requires covered entities to implement “*policies and procedures to address security incidents,*” which are defined as “*attempted or successful unauthorized access, use, or disclosure, modification, or destruction of information or interference with system operations in an information system*”¹⁶. This standard entails one specific requirement that pertains legally to clinical scribes:
 - ▶ Covered entities are required to “***identify and respond to suspected or known security incidents***; *mitigate, to the extent of practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes*”¹⁶. If you witness or suspect that you or someone you know may be involved in a security incident, your healthcare organization’s policies will likely require that you report this incident to the facility’s assigned security official(s).
- **Evaluation:** This standard requires covered entities to “*perform periodic technical and nontechnical evaluation[s], based initially upon the standards implemented under [the Security Rule] and subsequently, in response to environmental or operations changes affecting the security of ePHI...*”¹⁶ In your role as a clinical scribe, you will be subject to your facility’s periodic technical and nontechnical security evaluations.

Physical Safeguards

HIPAA’s Security Rule sets the following **Physical Safeguard Standards**, which legally apply to all Clinical Scribes:

- **Workstation Use:** Workstations are defined as “*electronic computing device(s), for example laptop or desktop computer[s], [computers on wheels], or any other device[s] that perform similar functions, and electronic media stored in their immediate environment[s]*”¹⁷. This standard requires covered entities to “*implement policies and procedures that specify the proper functions to be performed, the [way] those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI*”¹⁷.
- ▶ Your facility may implement policies that prohibit your from accessing social media on a facility workstation. Your facility may implement policies that prohibit the use- or

presence of personal electronic devices (such as cellular phones or iPads), food, or drink in your workstation environment. Failure to comply with such policies will be in direct violation of the HIPAA Security Rule.

- **Workstation Security:** This standard requires covered entities to “*implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users*”¹⁷.
- **Device and Media Controls:** Electronic media is defined as “*electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card*”¹⁷. This standard requires covered entities to “*implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI, into and out of a facility, and the movement of these items within the facility*”¹⁷. This standard entails four implementation specifications that include:
 - ▶ Device and Media Disposal
 - ▶ Media Re-Use
 - ▶ Accountability
 - ▶ Data Backup and Storage

These specifications and their legal relation to clinical scribes are addressed in Chapter 5.

Technical Safeguards

HIPAA’s Security Rule sets the following **Technical Safeguard Standards**, which legally apply to all Clinical Scribes:

- **Access Control:** Access is defined as “*the ability or means necessary to read, write, modify, or communicate data/information or otherwise use any system resource*”¹⁸. This standard requires covered entities to “*implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in [the Administrative Safeguards Information Access Management Standard]*”¹⁸. This standard specifies one implementation requirement that applies legally to the medical scribe role:
 - ▶ **Unique User Identification:** Covered entities are required to “*assign a unique name and/or number for identifying and tracking user identity*”¹⁸. As a clinical scribe, you will receive individual user identification information from your healthcare organization that pertains specifically to your role as a clinical scribe. You must only use this unique

user identification in your role as a clinical scribe. You may not use identification information assigned to other individuals or to other roles that you may hold within your facility to perform your duties as a clinical scribe. You may not share your user identification information with anyone else or allow anyone else to access ePHI using your user identification information.

- **Audit Controls:** This standard requires covered entities to “*implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI*¹⁸.”
 - ▶ All ONC-certified health information technology (CHIT) contains auditory controls.
 - ▶ It is critically important for critical scribes to understand that **all clinical scribe activity performed in information systems containing ePHI (such as electronic health record systems, EHRs) will be recorded and examined.**
- **Integrity:** Integrity is defined as “*the property that data or information have not been altered or destroyed in an unauthorized manner*¹⁸.” This standard requires covered entities to “*implement policies and procedures to protect ePHI from improper alteration or destruction*¹⁸.” This standard includes one specific implementation requirement that apply legally to the medical scribe role:
 - ▶ Covered entities must “*implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in any unauthorized manner*¹⁸.”
 - ▶ All CHIT contains auditory controls and ePHI integrity is often maintained through EHR audits.
 - ▶ The creation-, alteration-, and deletion of medical records all have the ability to compromise ePHI integrity. Therefore, **it is critically important for clinical scribes to understand the policies and procedures regarding creation-, alteration-, and deletion of electronic medical records,** as addressed below.
- **Person or Entity Authentication:** This standard requires covered entities to “*implement procedures to verify that a person or entity seeking access to ePHI is the one claimed*¹⁸.”
 - ▶ This standard is often maintained through the use of uniquely identifiable information that is specific to only one individual, such as a PIN, password, smart card, key card, token, or biometric information (fingerprint, voice pattern, etc.) that is required in order for any individual to access any ePHI.

Organizational Requirements

HIPAA's Security Rule set the following **Organizational Requirements**, which apply legally to all Clinical Scribes:

- **Policies and Procedures:** This standard requires all covered entities to *"Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in [the Security Standards: General Rules, Flexibility of Approach]. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart¹⁹."*

The Health Information Technology for Economic and Clinical Health Act (HITECH)

In 2009, the **Health Information Technology for Economic and Clinical Health Act (HITECH)** was enacted under Title XIII of the American Recovery and Reinvestment Act (ARRA) of the same year^{20,21}. HITECH provides a set of policies, regulations, and standards that promote "**Meaningful Use**" of certified health information technology (CHIT) based on NAM and ONCHIT guidelines for "core functions" of HIT and EHR systems^{22,23}.

The organizational structure of HITECH is reviewed in Appendix A.VIII. In general, HITECH is organized into different subtitles. Subtitles A and D are legally pertinent to the clinical scribe role, as outlined below²⁴.

- **Subtitle A – Promotion of Health Information Technology**
 - ▶ Part 1 – Improving Health Care Quality, Safety, and Efficiency
 - Title XXX – Health Information Technology and Quality
 - Sections 3001 – 3009 introduce the Office of the National Coordinator for Health Information Technology (ONCHIT); HIT Policy- and Standards Committees; HIT adoption and implementation processes; and "application and use of adopted standards and implementation specifications²⁴."

- ▶ Part 2 – Application and Use of Adopted Health Information Technology Standards; Reports.
- **Subtitle D – Privacy**
 - ▶ Part 1 – Improved Privacy Provisions and Security Provisions
 - ▶ Sections 13401 – 13411 address issues that are largely covered in the HIPAA Privacy Policy, but in reference to meaningful use of HIT.
 - **Section 13411. Provides the following statement on Audits:**

“The Secretary shall provide for periodic audits to ensure that covered entities and business associates that are subject to the requirements of [The HIPAA Privacy and Security Rules, 45 CFR 164 Subparts C and E] ... comply with such requirements²⁴.” The relevance of EHR Audits are addressed further below.

HIPAA and HITECH Final Enforcement Rules & Breach Notification Rules

In 2009, the U.S. Department of Health and Human Services enacted the **Breach Notification Rule** into law under Title 45 the Code of Federal Regulations (CFR) § 164.400-414^{25,26}. This rule established policy regulations and requirements regarding the way in which covered entities and business associates respond to possible and actual security breaches. The Breach Notification Rule is reviewed in Appendix A.VIII.

Under the Breach Notification Rule, Clinical Scribes are responsible for notifying Scribe Supervisors and appropriate HIPAA Security Personnel (associated with the covered entity and/or business associate group of employment or contract) if there is any concern that a breach of security has occurred. This also pertains to any suspected or possible violations of the HIPAA Privacy and Security Rules.

Between 2006 - 2013 **HIPAA and HITECH Enforcement Rules** were issued and finalized by the U.S. Department of Health and Human Services that built upon the Social Security Act's code for civil monetary penalties for improperly filed medical service claims. **The HIPAA and HITECH Enforcement Rules established investigative procedures and civil monetary penalties for HIPAA and HITECH violations^{20,21,27,28}**. These Rules are reviewed in Appendix A.VIII.

All individuals who access PHI of any kind are subject to the investigative procedures and civil monetary penalties set forth by these rules, in addition to those procedures and penalties set forth by each specific covered entity.



SuperScribe Tip:

- The HIPAA and HITECH Final Enforcement Rules establish investigative procedures and civil monetary penalties associated with HIPAA and HITECH violations.
- All individuals who access protected health information (PHI) of any kind are subject to the investigative procedures and civil monetary penalties set forth by the HIPAA and HITECH Final- and Enforcement Rules.
- All individuals who access PHI are also subject to the investigative procedures, sanctions, and penalties set forth by each specific covered entity.

CMS Requirements for Medical Documentation

A variety of different regulations exist regarding the criteria that medical records must meet in order to be used for financial-, business-, and legal purposes. For example, in order for a healthcare provider or covered entity (such a hospital or clinic) to submit a payment claim to the Center for Medicare & Medicaid Services (CMS) to receive reimbursement for services provided to Medicare and Medicaid patients, the provider or entity must meet CMS' **Condition(s) of Participation (CoP)**.

CMS' CoPs include a variety of standards that vary depending on the participant. For example, hospital CoPs differ somewhat from those that apply to individual providers and private practices/clinics.

CMS' CoP's regarding **Medical Record Services** and **Clinical Record Content** are provided below as examples of these federal regulations that pertain to the ability of a medical record to be used in a business/financial and legal capacity. Module III covers many of these regulations in greater depth.

Where medical records are used to track medical practices, services, and business transactions for non-Medicare/Medicaid patients, separate requirements exist, which are addressed in the sections on "Business Records" and "Legal Health Records" in Chapter 19 below.

CMS' Legal Requirements for Hospital Medical Record Services and Content²⁹

Hospital CoP standards regarding medical record services pertain to **organization and staffing**, **form and retention of medical health records**, and **medical record content**, as outlined in the Code of Federal Regulations (CFR) Section on “Medical record services” (42 § CFR 484.24(a-c))²⁹.

CMS' Conditions of Participation (CoPs) for hospital medical record services regarding **Organization and Staffing** (a) and **Medical Record Form and Retention** (b) echo policies outlined in HIPAA and HITECH (in Chapter 5 of this manual) and require hospitals to:

- (a) “Employ adequate personnel to ensure prompt completion, filing, and retrieval of records²⁹.”
- (b) “Maintain a medical record for each inpatient and outpatient that must be:
 - ▶ Accurately written
 - ▶ Promptly completed
 - ▶ Properly filed and retained
 - ▶ Accessible

[Additionally], the hospital must use a system of **author identification** and record maintenance that ensures the **integrity of the authentication** and protects the **security** of all record entries. [Additionally]:

- (1) Medical records must be **retained in their original or legally reproduced form** for a period of at least 5 years.
- (2) The hospital must have a system of coding and indexing medical records... that allows for **timely retrieval by diagnosis and procedure**, in order to support medical care evaluation studies.
- (3) The hospital must have a procedure for ensuring the **confidentiality** of the patient records. Information from or copies of records may be released only to authorized individuals, and the hospital must ensure that unauthorized individuals cannot gain access to or alter patient records. Original medical records must be released by the hospital only in accordance with Federal or State laws, court orders, or subpoenas²⁹.”

HIPAA & HITECH Compliance Influence the Legal Credibility of the Medical Record

CMS' CoPs for hospital medical record services echo many policies outlined in the **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**'s **Privacy- and Security Rules** and in the **Health Information Technology for Economic and Clinical Health Act (HITECH)**, as outlined above.

As a clinical scribe who assists in medical documentation, your compliance with HIPAA and HITECH policies can have an impact not only on you personally, but also on the authentication of the medical records you assist in documenting.

For example, if your medical documentation fails to meet HIPAA and HITECH standards, you may produce a medical record that cannot legally hold up in a court of law.

The requirements and standards that pertain to the ability of medical records to be used as business- and legal records are addressed further in Chapter 19 below.

CMS' Conditions of Participation (CoPs) for hospital medical record services regarding **Medical Record Content** (42 § CFR 484.24(c))²⁹ provide a **financial-legal definition for medical records** that require medical records to justify the **medical necessity** for all services rendered by providing "information to

- ▶ *justify admission and continued hospitalization [or care]*
- ▶ *Support the diagnosis*
- ▶ *Describe the patient's progress and response to medications and services.*
- *"(1) Additionally all patient medical record entries must be:*
 - ▶ *Legible*
 - ▶ *Complete*
 - ▶ *Dated*
 - ▶ *Timed*
 - ▶ *Authenticated*
 - *in written or electronic form by the person responsible for providing or evaluating the service provided, consistent with hospital policies and procedures*

- *(i) all orders, including verbal orders, must be dated, timed, and authenticated promptly by the ordering practitioner*
- *(2) All records must document the following, as appropriate:*
 - ▶ *(i) Evidence of:*
 - *(A) A **medical history** and **physical examination** that are:*
 - ◆ *completed and documented no more than 30 days before- or 24 hours after admission or registration*
 - ◆ *placed in a patient's medical record within 24 hours after admission or registration...*
 - *(B) An **updated examination** of the patient, including any changes in the patient's condition, when the medical history and physical examination are completed within 30 days before admission or hospital registration.*
 - ◆ *Documentation of the updated examination must be placed in the patient's medical record within 24 hours after admission or registration...*
 - ▶ *(ii) **Admitting diagnosis***
 - ▶ *(iii) Results of all **consultative evaluations** of the patient and appropriate findings by clinical and other staff involved in the care of the patient*
 - ▶ *(iv) Documentation of **complications**, hospital acquired infections, and unfavorable reactions to drugs and anesthesia*
 - ▶ *(v) Properly executed **informed consent** forms and procedures and treatments specified by the medical staff, or by Federal or State law if applicable, to require written patient consent*
 - ▶ *(vi) Additional documentation of **service and care**, including:*
 - *All practitioners' orders*
 - *Nursing notes*
 - *Reports of treatment*
 - *Medication records*
 - *Radiology*
 - *Laboratory reports*
 - *Vital signs*
 - *Other information necessary to monitor the patient's condition*

- ▶ (vii) **Discharge summary** with outcome of hospitalization, disposition of care, and provisions for follow-up care
- ▶ (viii) **Final diagnosis** with completion of medical records within 30 days following discharge²⁹.”

CMS' Legal Requirements for Clinical Record Content for specialized providers³⁰

CMS' Condition of Participation (CoP) standards for *clinics and specialized providers* are similar to those offered above for hospitals, with some differences pertaining to the **Clinical Records Content** standards (as outlined in 42 § CFR 485.721(b))³⁰.

CMS' Conditions of Participation (CoPs) for medical record services regarding **clinical record content** for *clinics and specialized providers* (42 § CFR 485.721(b)) requires clinical records to contain “sufficient information to:

- Identify the patient clearly
- Justify the diagnosis(es) and treatment [Medical Necessity]
- Document the results accurately³⁰.”

All clinical records must also contain the following general categories of data:

- “(1) Documented evidence of the assessment of:
 - ▶ The needs of the patient
 - ▶ An appropriate plan of care
 - ▶ The care and services furnished
- (2) Identification data and consent forms
- (3) Medical History
- (4) Report of physical examinations, if any
- (5) Observations and progress notes
- (6) Reports of treatments and clinical findings.
- (7) Discharge summary including final diagnosis(es) and prognosis³⁰”

Note: these standards apply to arrangements for physical therapy and speech pathology services

to be performed by other than salaried organization personnel³⁰. However, they are presented here to offer an example of a valid *legal standard* on medical record content.

Similar to CMS' Condition of Participation (CoP) for hospitals, CMS's CoP standards regarding Clinical Records for specialized providers (42 § CFR 485.721(a-f) also offer standards regarding: (a) Protection of clinical record information; (c) Completion of records and centralization of reports; (d) Retention and preservation; (e) Indexes; (f) Location and facilities.³⁰

Review & Assessment

Recommended Resources

1. U.S. Dept. of Health and Human Services' HIPAA & HITECH Summary
 - <https://www.hhs.gov/hipaa/for-professionals/index.html?language=en>
 - Includes summaries of: HIPAA Privacy and Security Rule,; Breach Notification Rule(s), Compliance & Enforcement Rule(s), Administrative Rules, Special Topics (including HITECH).
2. Cornell Law School's Electronic Code of Federal Regulations (e-CFR)
 - <https://www.law.cornell.edu/cfr/text/42/chapter-IV/subchapter-G>
 - Full Code of Federal Regulations
 - Includes full Code of Federal Regulations, including CMS' CoPs reviewed in this chapter.
3. Resource Tab of the CSAT Website (www.scribeACCELERATOR.com)

Review

1. Medical records can be used in a court of law. Therefore, all interactions with medical records and patient health information have the potential to constitute access to legal evidence. In order to protect the legal authentication of a medical record, it is important for all clinical scribes to understand- and comply with all organizational-, state-, and federal policies pertaining to the use and access of protected health information (PHI) and medical documentation. Important regulatory policies that protect the legal authentication of a medical record include:
 - The Health Information Portability and Accountability Act (HIPAA), including:
 - ▶ The HIPAA Privacy Rule
 - ▶ The HIPAA Security Rule:
 - Administration Safeguards
 - Physical Safeguards
 - Technical Safeguards
 - Organizational Requirements

- The Health Information Technology for Economic and Clinical Health Act (HITECH), including:
 - ▶ Subtitle D - Privacy
 - 2. **HIPAA** provides a set of standards regarding the use and disclosure of **protected health information (PHI)**. Three concepts that are central to HIPAA policies include^{1,2}:
 - Individually identifiable health information
 - Protected health information (PHI)
 - The “Minimum Necessary” use of PHI
 - 3. **HIPAA’s Privacy Rule** requires all healthcare providers and organizations to provide all employees with the following requirements:
 - Written Privacy Policies and Procedures
 - Access to Privacy Personnel
 - Training, Management, and Enforcement on- and of its privacy policies and HIPAA Compliance
 - Data Safeguards, such as individual login authorization and information
- Independent clinical scribes are legally responsible for compliance with the Privacy regulations set forth by HIPAA at the organizational and federal levels.
- 4. **HIPAA’s Security Rule** provides a set of standards regarding the use and disclosure of **electronic protected health information (ePHI)**. The Security Rule provides standards regarding the following areas:
 - Administrative Safeguards
 - Physical Safeguards
 - Technical Safeguards
 - Organizational Requirements
 - 5. **HIPAA’s Security Rule Administrative Safeguard Standards** require covered entities to implement information system activity reviews, which must include “*procedures to regularly review records of information system activity, such as audit logs, access reports, and security incidence tracking reports*”³.

- As a clinical scribe, it is important to be aware that all attempts to access any ePHI will be monitored, recorded, retained, and regularly reviewed.

6. **HIPAA's Security Rule Technical Safeguard Standards** require covered entities to implement policies and procedures that enable:

- Unique user identification
- Audit review
- Integrity of Medical Documentation

In your role as a clinical scribe:

- All of your activity within an information system that contains or uses ePHI will be recorded and examined regularly
- You are responsible for identifying your organization's policies regarding altering or deleting any ePHI. Failure to comply with these policies may constitute tampering- or destroying legal evidence.

7. Subtitle D of HITECH reinforces HIPAA Privacy and Security standards and:

- Requires all covered entities to use certified electronic health record systems (CEHRS)
- All CEHRS are required to contain mechanisms to recording and reviewing information system activity, such as:
 - ▶ Audit Logs
 - ▶ Access Reports
 - ▶ Security incident tracking reports.
- The Secretary of the Department of Health and Human Services is responsible for ensuring all user activity within a CEHR is regularly reviewed for HIPAA and HITECH compliance

In your role as a clinical scribe, all of your activity within an electronic health record system will be recorded, retained, and regularly reviewed.

8. HIPAA and HITECH compliance influence the legal credibility of the medical record.

9. Medical records are often used by businesses as financial documents. The Center for Medicare and Medicaid Services (CMS) has specific standards that must be met in order for a medical record to be legally used as a business/financial document to support claims payments. The CMS Conditions of Participation standards relate to:
- Organizational staffing
 - Medical Record Form/Content
 - Medical Record Retention

Assessment

1. What is Individually identifiable health information? Provide 3 examples of how you might interact with individually identifiable health information in your role as a clinical scribe.
2. What is protected health information? Provide 3 examples of how you might interact with PHI in your role as a clinical scribe.
3. What is the “Minimum Necessary” Rule? How does it apply to the way that you can- and cannot use PHI in your role as a clinical scribe?
4. What is an audit trail and how does it relate to your interaction with ePHI?
5. Who are the privacy personnel at the healthcare facility you work with/for? How can you access these individuals? Provide 3 examples of situations in which you may need to interact with your facility’s privacy personnel.
6. HIPAA’s Security Rule requires that you receive training-, management-, and enforcement on- and of the Privacy Policies developed by the administration staff at the healthcare organization your work for/with. How can you ensure that you receive HIPAA training? How will your HIPAA compliance be managed and enforced by the healthcare organization you work with?
7. What are the data safeguard policies implemented by your healthcare organization regarding individual login authorization and information?
8. Why is it legally important to follow proper procedures when creating, accessing, altering, editing, or deleting medical records?



19

The Legal Medical Record

Clinical-, Business-, and Legal Health Record Documentation

Chapter 1 of this manual identifies the **4 Pillars of Medical Documentation**, which include:

- General & Regulatory/Policy Aspects
- Medical Aspects
- Financial Aspects
- Legal Aspects

Module I of this manual introduces policies, procedures, and federal regulations that legally pertain to the clinical scribe role (including HIPAA and HITECH regulations). **Module II** of this manual covers the medical aspects of documentation and focuses on the clinical health record, which health care providers use for medical purposes. **Module III** of this manual covers the financial aspects of medical documentation, and focuses on the ways in which medical records are used by insurance companies and billing agencies for financial purposes. Here, (**Module IV**) we focus on the **legal aspects of medical documentation**. In addition to providing medical and financial records, medical records also serve as legal documents that may be used in court to support or deny claims of malpractice, quality care delivery, or improperly filed claims for medical services³¹.

To illustrate this concept, we will review different functions of medical documentation as they pertain to patient care, public health, financial and business record-keeping, and legal documentation. We will also provide some additional terminology that can be useful in distinguishing the regulatory-, clinical-, financial-, and legal aspects of medical documentation – and medical records themselves – from one another³².

Patient Care Documentation

Recall your last encounter with your own health care provider. Your provider may have referenced records in your chart that dated back 10- or even 15 years. One purpose of the medical record is to provide a comprehensive history of illnesses, treatments, surgeries, or other health care milestones that other practitioners will **need to know** in order to provide you with the highest possible quality of health care^{33,34}. A comprehensive patient history enables a continuum of short- and long-term care among a variety of providers and settings.

For example, if your primary care physician refers you to a specialist, the specialist will require access to your previous medical records to develop an appropriate plan of care that is not

redundant. The specialist will need to understand the reason for your referral, the diagnostic studies that have already been conducted, and the findings of those studies. This information will enable the physician to make educated medical decisions regarding your treatment and care plan. Your medical records will provide the information your practitioners need to know about you in order to determine the most appropriate plan of care.

Medical records provide the medium by which practitioners can communicate with one another to provide complete and collaborative patient care.



SuperScribe Application: The Clinical Medical Record (CMR)

The clinical medical record pertains to the medical record as used by clinicians and patients, and documents the clinical aspects of patient care.

CMS' Evaluation and Management Services Guide (introduced in Module III) provides a competent definition:

A chronological report of the care a patient receives, which “[records] pertinent facts, findings, and observations about the patient’s health history ... to help physicians and other health care providers evaluate and plan the patient’s immediate treatment and monitor the patient’s health care over time⁷.”

This definition emphasizes the clinical/medical purpose and function of the medical record “to help physicians and other health care providers evaluate and plan the patient’s immediate treatment and monitor the patient’s health care over time,” which focusses on the clinical aspects of patient care.

Public Health Documentation

Medical records also provide a medium by which statisticians and epidemiologists can access information reported to them or their associated agencies for the benefit of the community as a whole. For example, if a specific demographic population demonstrates increased incidence of infection related to a certain communicable disease, this information can be extracted from the medical records of the affected patients within the affected demographic in order to alert health agencies or the community at large.

Statistical data may also be extracted from medical records for the purposes of research or for continuing education objectives. Statistical information in medical records may be used to identify **health risk factors** associated with various diseases, or health factors associated with increased patient prognosis following a specific type of diagnosis or intervention. Monitoring health care trends through medical record information provides vital assistance to our health care community.

SuperScribe Application:

Chapter 12 in Module III on **Meaningful Use** discusses the Stage 1 Menu- and Stage 2 Core Objectives of **submitting electronic data to immunization registries and public health agencies**.

Recently, medical records were used to identify geographic regions in the U.S. with high incidence of West Nile Virus outbreak; public health officials were then able to eliminate the mosquito populations in these areas to prevent further outbreaks. In this way, medical records provide valuable resources to public health officials who use medical documents to protect public health.

Financial Documentation

In addition to its clinical documentation, the medical record provides financial documentation upon which **payments are rendered** for health care services (as addressed in Module III). Just as a restaurant bill provides a list or receipt of all items ordered (and received) at a particular restaurant, a medical record outlines all services, tests, and patient care measures provided to a patient during a patient's encounter with a health care provider.

Coding services translate each patient's medical record into an itemized list of services rendered to the patient during an encounter. Billing agencies may then send this claim to a patient's insurance company – or to the patient – to receive payment for the **services rendered**.

At a restaurant, a customer is likely to notice if charged for an extra item – such as a beverage – that the customer did not order or receive. If a restaurant were to provide you with a piece of cake that you did not order, but were to later charge you for that item; you may dispute the payment. Likewise, insurance companies and government agencies like CMS closely scrutinize medical claims to ensure **accuracy and medical necessity** of all items ordered and billed. As health care costs continue to rise, the importance of thorough and accurate medical documentation is likely to continue to grow as well.

SuperScribe Application: The Designated Record Set (DRS) for Medico-Business Documentation:

Module I provides a distinction between the electronic medical record and the electronic health record:

- **Electronic Medical Record (EMR)** constitutes the patient's health record relative to just one facility (including provider notes from all of a patient's visits at one particular facility, such as the patient's primary care clinic)³.
- **Electronic Health Record (EHR)** "a summary of health events (usually drawn from several EMRs) and may consist of the elements that are eventually shared in a national EHR³." The EHR thus constitutes the patient's entire health record, which is easily transferrable between medical facilities and other sources^{8,9}.

A similar distinction exists between the clinical medical record and the **designated record set (DRS)**. The designated record set is defined in title 45 of the code of federal regulations (CFR) (45 CFR § 164.501) as:

"(1) A group of records maintained by or for a covered entity that is:

- (i) The medical records and billing records about individuals maintained by or for a covered health care provider;*
- (ii) The enrollment, payment, claims adjudication, and case or medical management record system maintained by or for a health plan;*
- (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.*

(2)...any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity¹⁴."

This definition emphasizes the role of the medical record as a **business document** that can be used by healthcare entities to track *financial transactions* (such as billing items and releases) as well as medical services. Where incidences of malpractice or legal affairs are concerned, this definition provides insight into the ability of the medical record to serve not only as a clinical document, but also as a business document (and as a legal one, as addressed below).

Legal Documentation

In addition to its medical and financial implications, the medical record also functions to protect the legal interests of patients and health care providers alike. Unfortunately, not all health care services result in positive outcomes; perhaps as a result, **medical malpractice lawsuits** have become an accepted part of the health care system. Many health care practitioners consider the prospect of a malpractice lawsuit an unavoidable “hazard of the trade;” however, malpractice lawsuits can also help to establish patient care standards and prevent the occurrence of negative outcomes.

In the event of a malpractice lawsuit, a medical record will be admitted into evidence and closely scrutinized by attorneys on both sides of a case. Most lawsuits typically ensue several **years** after a provider in question has treated a patient. When a provider involved in a plaintiff's care is called to the witness stand, the provider may not be able to recollect a specific patient's case from memory. The provider is likely to review the information included in the patient's medical record prior to testifying in that patient's case. Often the medical record provides the only reliable source of information on a patient's encounter with a particular practitioner on a particular date. **Depending on the quality of its documentation, a medical record can provide a saving grace or a legal nightmare for a health care provider involved in a malpractice lawsuit.**



SuperScribe Tip:

As with any type of lawsuit, malpractice lawsuits require evidence of malpractice in order to establish a cause of action. In the health care system, the medical record provides documentation – evidence – that can be used to establish cause of action in a court of law – or dispute such cause.

The Legal Business Record and The Legal Health Record (LHR)

A variety of different regulations exist regarding the criteria that medical records must meet to be used for financial-, business-, and legal purposes. For example, healthcare providers and organizations who service Medicare and Medicaid patients must meet CMS Standards regarding **Medical Record Services** and **Clinical Record Content** in order to qualify for CMS reimbursement, as identified in Chapter 18^{29,30}.

Where medical records are used to track medical practices, services, and business transactions for *non-Medicare/Medicaid patients*, separate requirements exist, which are addressed below.

The Business Record

The American Health Information Management Association defines a **business record** as: “A record prepared and kept in the regular course of business that can legally be received into evidence in court if the method of record keeping conforms to certain established guidelines:

- “The record was made in the regular course of business
- The entries in the record are made promptly
- The entries were made by the individual within the enterprise with first-hand knowledge of the acts, events, conditions, and opinions
- Process control and checks exist to ensure the reliability and accuracy of the record
- Policies and procedures exist to protect the record from alteration and tampering
- Policies and procedures exist to prevent loss of stored data³⁵.”

This definition emphasizes the importance of compliance with federal regulations such as the Healthcare Insurance Portability and Accountability Act (HIPAA)’s Privacy and Security Rules, and the Health Information Technology for Economic and Clinical Health Act (HITECH) (addressed in Chapters 5 and 18) to preserve the integrity of the medical record as a business- and legal document.

The Legal Health Record

AHIMA offers another definition of the medical record in reference to its legal capacity – that of the **Legal Health Record (LHR)**. AHIMA defines the **Legal Health Record (LHR)** as a medical record that is “generated at or for a healthcare organization as its business record and is the record that would be released upon request³⁵.”

By these definitions, the designated record set (DSR), business record, and legal health record (LHR) are essentially one in the same: the designated record set provides documentation of clinical and business services, and if the medical record follows certain regulations it may also be used to verify these services in a court of law.

In a recent Health Care Compliance Association (HCCA) webinar on “The Medical Record and Its Role in Litigation” Sean McKenna, JD, and Rachel Rose, JD, MBA describe the Legal Health Record as providing documentation of³²:

- **Clinical Care** (including quality standards and compliance)
- **Claims submitted to third-party payers** (thus providing financial documentation)
- **Services that could be utilized as a basis of testimony** (including other legal aspects)

Review& Assessment

Recommended Resources

1. Health Care Compliance Association Website and Resources

- <https://www.hcca-info.org/>
- Index of Valuable Health Care Compliance Resources, including: McKenna SR, Fose, RV. The Medical Record and Its Role in Litigation [Webinar]. <http://www.hcca-info.org/>. Health Care Compliance Association; 2018³².

2. American Health Information Management Association (AHIMA) Website

- <http://www.ahima.org>
- Contains resources for Health Information Management (HIM) Certifications, Training & Education, and the Journal of AHIMA
- AHIMA Library Index: <http://library.ahima.org/>

3. “The Legal Process and Electronic Health Records” (Bartschat *et al.*, 2005)³⁵: <http://library.ahima.org/doc?oid=59559#.XLXzD-tKifV>

4. Cornell Law School’s Electronic Code of Federal Regulations (e-CFR)

- <https://www.law.cornell.edu/cfr/text/42/chapter-IV/subchapter-G>
- Full Code of Federal Regulations
- Referenced in this Chapter (from the CFR):
- Definitions (45 CFR § 164.501)
- Minimum Necessary Requirement (45 CFR § 164.502(b), 164.514(d))
- CMS Conditions of Participation (42 CFR § 482.24; 42 CFR § 485.721)

5. U.S. Dept. of Health and Human Services’ HIPAA & HITECH Summary

- <https://www.hhs.gov/hipaa/for-professionals/index.html?language=en>
- Includes summaries of: HIPAA Privacy and Security Rule,; Breach Notification Rule(s), Compliance & Enforcement Rule(s), Administrative Rules, Special Topics (including HITECH).

6. Resource Tab of the CSAT Website (www.scribeACCELERATOR.com)

Review

1. The three main purposes of a patient's medical record are to provide:

- Medical documentation regarding patient care
- Financial documentation
- Legal documentation

2. The following definitions can help to distinguish different aspects of the Medical Record:

- **Clinical Health Record:**

"A chronological report of the care a patient receives, which "[records] pertinent facts, findings, and observations about the patient's health history ... to help physicians and other health care providers evaluate and plan the patient's immediate treatment and monitor the patient's health care over time⁴."

- **Designated Record Set:**

"(1) A group of records maintained by or for a covered entity that is:

- I. The medical records and billing records about individuals maintained by or for a covered health care provider;*
- II. The enrollment, payment, claims adjudication, and case or medical management record system maintained by or for a health plan;*
- III. Used, in whole or in part, by or for the covered entity to make decisions about individuals.*

(2)...any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity⁵."

- **Business Record:**

"A record prepared and kept in the regular course of business that can legally be received into evidence in court if the method of record keeping conforms to certain established guidelines:

- ▶ *"The record was made in the regular course of business*
- ▶ *The entries in the record are made promptly*

- ▶ *The entries were made by the individual within the enterprise with first-hand knowledge of the acts, events, conditions, and opinions*
- ▶ *Process control and checks exist to ensure the reliability and accuracy of the record*
- ▶ *Policies and procedures exist to protect the record from alteration and tampering*
- ▶ *Policies and procedures exist to prevent loss of stored data⁶.*

- **Legal Health Record:**

Medical record that is “*generated at or for a healthcare organization as its business record and is the record that would be released upon request⁶.*”

Assessment

1. Explain the importance of the medical record and the possible negative outcomes that can result from inaccurate or incomplete documentation.
2. What are 5 ways that you as a clinical scribe can ensure the medical record you create is able to be used by your provider or healthcare organization as a clinical record?
3. What are 5 ways that you as a clinical scribe can ensure the medical record you create is able to be used by your provider or healthcare organization as a financial or business record?
4. What are 5 ways that you as a clinical scribe can ensure the medical record you create is able to be used by your provider or healthcare organization as a legal record?



20

Medicolegal Documentation (I): Audits & Amendments

Legal Health Record Documentation

Chapters 17 and 19 convey the concept that a medical record may be used in a court of law as a legal document. The sections on **CMS' Conditions of Participation** standards for documentation (Chapter 18) and the American Health Information Management Association (AHIMA)'s definitions of the **Business Record** and the **Legal Health Record** (Chapter 19) provide examples of regulatory requirements

that medical documents must meet to demonstrate legal authenticity. When considering the medical record as a legal document, it is important to consider each medical record as possible piece of legal evidence. Accordingly, any interaction that you have with a medical record has the potential to constitute an interaction with legal evidence. When you create a medical record, you are creating a potential artifact that may be used as evidence in a court of law. If you edit or delete a medical record (or any portion of a medical record) that is called into legal question, this may constitute **tampering with- or destroying legal evidence**, which holds important legal ramifications.

Chapter 18 highlights some important aspects of HIPAA and HITECH that pertain legally to the clinical scribe role, especially in light of the possibility of any medical record being used as evidence in a court of law:

- **The HIPAA Security Rule** requires covered entities to implement **audit control mechanisms** that “record and examine [all] activity in information systems [containing or using] ePHI¹⁸” and to “**regularly review records of information system activity**, such as audit logs, access reports, and security incident tracking reports¹⁶.”
- **The HITECH Privacy Rule** (Subtitle D) requires audit review at the Federal level which is to be conducted by the Secretary of Health and Human Services “to ensure that covered entities and business associates ...[comply with HIPAA Privacy and Security Standards]²¹.”
- **The HIPAA Security Rule** also requires covered entities to **protect the integrity of ePHI** and all medical and health records by “[implementing] policies and procedures to protect ePHI from improper alteration or destruction¹⁸.” Specifically, covered entities are required to “implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in any unauthorized manner¹⁸.”

In the same way that facilities have surveillance cameras that can be used as evidence in a court of law for legal cases, health record systems have internal surveillance cameras that track all activity and can also be used in a court of law. Therefore, it is of critical legal importance that all clinical scribes interact with all ePHI within the regulatory requirements HIPAA, HITECH, and the specific administrative policies of the scribe's Healthcare Facility.

This point is eloquently articulated by Michelle Dougherty, RHIA, CHP and director of practice leadership for the American Health Information Management Association (AHIMA) in her 2019 article “Identifying Key Functions that Support a Legal Record³⁶” which can be accessed online at <http://bok.ahima.org/doc?oid=77552#.XGtVQ89Khp9>. Dougherty states:

“An EHR’s security practices and functions have the potential to play a role in litigation because they support the integrity and trustworthiness of the health record maintained within the system. In litigation, [an] organization’s security practices ... [and] adherence to applicable security laws (such as HIPAA) and standards (such as the Joint Commission) may also be called into question³⁶.”

For this reason, we provide some additional information on a few key legal aspects of electronic documentation that support a legal record: Audit Trails, Electronic Record Discovery, and EHR Amendments.

Audit Trails and Electronic Record Discovery

In her 2019 article “Identifying Key Functions that Support a Legal Record,” Dougherty identifies several key functions that support a legal record, three of which we will highlight below:

- **Auditable Records:**
 - ▶ **Functional Description:** *“Provide audit capabilities for system access and usage indicating the author, the modification (where pertinent), and the date and time at which a record was created, modified, viewed, extracted, or deleted. Auditable records extend to information exchange, to audit of consent status management, and to entity authentication attempts. Audit functionality includes the ability to generate audit reports and to interactively view change history for individual health records or for an EHR system³⁶.”*
 - ▶ **Legal Rationale:** *“The audit functionality provides traceability to show the activities ‘behind the scenes.’ With traceability comes trustworthiness in the electronic records to be used in legal proceedings³⁶.”*

- **Data Retention, Availability, and Destruction:**

- ▶ **Functional Description:** *“Retention, ensure availability, and destroy health record information according to scope of practice, organizational policy, or jurisdictional law³⁶.”*
- ▶ **Legal Rationale:** *“Adherence to organizational retention and destruction policies that comply with jurisdictional law is critical in legal proceedings to prevent accusations of spoliation of evidence and establish that the organization destroyed records as part of their good faith practices. Organizations must develop a policy which defines their official medical record for official disclosure purposes (reimbursement, litigation, regulatory, etc.). The EHR system must be able to support the retrieval of the elements the organization considers part of their legal medical record. This includes business context data (such as metadata) retained by the system which may provide context of when a record was created, by whom, etc³⁶.”*

- **Record Preservation:**

- ▶ **Functional Description:** *“Preserve data from normal destruction practices including a duty to preserve material evidence when the organization reasonably should know that the evidence (health record information) may be relevant to anticipated litigation³⁶.”*
- ▶ **Legal Rationale:** *“Organizations have a duty to preserve information that is or could be relevant to a legal proceeding whether litigation is threatened (the potential for) or impending. Systems must provide the ability for users to place a legal hold on electronic health information (suspend their normal destruction practices for all potentially relevant information) and prevent from loss, destruction, alteration, or unauthorized use³⁶.”*

In light of these three key functions of most EHR systems, Patricia McCartney, PhD, RN, FAAN – a Clinical Professor at The State University of New York School of Nursing – wrote an informative article on “Audit Trails and Electronic Record Discovery³⁷” which can be accessed online at:

- <https://insights.ovid.com/pubmed?pmid=19104323>
- https://journals.lww.com/mcnjournal/Citation/2009/01000/Audit_Trails_and_Electronic_Record_Discovery.14.aspx

In her article, McCartney echoes Dougherty’s definition of an audit report as: *“a chronological review of patient data, alerts, and entries in the EMR [that] can be used to identify breaches in security and provide evidence for legal review,”* (Dougherty, 2008 as cited in McCartney, 2009)³⁷. McCartney adds that:

- *“The audit function records:*
 - ▶ *The identity of each information system user*
 - ▶ *The date and time of access*
 - ▶ *What the user did (view the record, create an entry, edit an entry, or delete an entry).*
- *Because user access is recorded, the audit provides nonrepudiation, meaning that the user cannot deny accessing the EMR³⁷.”*

It is critically – and legally – important for all scribes to be aware that each interaction with any protected health information or medical/health record may constitute an interaction with legal evidence in a court of law. Therefore, the following section will provide some guidelines on medical record documentation from a legal standpoint.

Documentation Amendments

All user access to any ePHI – including electronic medical records and health records – is recorded, preserved, retained, and subject to auditory review and use in court. Altering any medical record can thus constitute tampering with legal evidence. Therefore, it is important for scribes to understand how to appropriately amend medical documentation, in situations where amendments are required.

Trish Lugtu, BS, CPHIMS, CHP, and associate director of research for a medical professional liability insurance company, provides the following statement regarding amendments to medical record documentation:

“Amendments describe a range of alterations that are intended to clarify information. The processes for amending documentation are ...complex with EHRs... as the nuances are captured behind the scenes in metadata, which increases the importance of clarifying how each [type of amendment] is defined³⁸.”

According to the American Health Information Management Association (AHIMA)’s Electronic Health Record Toolkit³⁹, all healthcare organizations are required at the federal level to establish policies and procedures on how to change the health record in such cases where changes are required³⁹. AHIMA identifies 6 main types of changes – or amendments – that occur in medical documentation, and provides the following guidelines for policies regarding these amendment types³⁹:

- **Addendums:** According to AHIMA EHR Toolkit guidelines, addendums are the only

appropriate way to correct or revise a medical document once the document has a final sign-off³⁹. Methods to attach or connect addendums to an original document vary according to the EHR system being used, and officially, each healthcare organization is individually responsible for developing policies and procedures regarding how addendums are made in a health record^{38,39}. At a minimum, all addendums must include the date of documentation and must be completed according to the organization's documentation completion policies³⁸.

- **Corrections:** Corrections constitute changes to the medical or health record that are “intended to fix an inaccuracy in an entry³⁸.” According to AHIMA, *“organizations should have clear policy and procedure covering its system’s ability to issue documentation corrections. The policy and procedure should cover issuing corrections to a signed document, as well as ...to a document before it is signed³⁹.”* Organizations are also suggested to specify policy regarding *who* is allowed to make such corrections. Policies should also specify how to correct comingled records – such as when moving an entry from one patient to another – without breaching patient privacy³⁸.
- **Retractions:** Like corrections, retractions are used to correct invalid information or documentation made in error in reports that are already locked. Retractions can be crucial to enable appropriate medical decision making; however, they must also require strict policy enforcement, as they can constitute tampering with evidence. It is suggested that retractions require specific interventions from authorized personnel³⁹. In the event that retracted information is “hidden from general viewing,” it must remain archived and accessible³⁹.
- **Deletions:** Deletions completely eliminate information from an EHR. Most EHR systems do not allow total elimination of information, and organizations are also suggested to prohibit entry deletion^{38,39}. In the case that entry deletions are allowed, AHIMA and Lugu suggest that to ensure the integrity of the health record, clear policies and procedures be employed that include: controlling authorization for entry deletion; frequent staff- and audit monitoring, and tracking all deleted entries.
- **Late Entries:** Late entries refer to any entry that occurs outside the point of care. AHIMA suggests that organizations clearly define how late entries are made within a facility's given EHR system, and the time frame in which late entries may be inserted³⁹. Additionally, organizational staff should understand the way in which late entries are tracked within an EHR system.

- **Re-sequencing or Reassignment:**

- ▶ **Re-sequencing** refers to “the process of moving a document from one location in the EHR to another within the same episode of care, such as a progress note that was linked to the wrong date⁴⁰.”
- ▶ **Reassignment** refers to “the process of moving one or more documents from one episode of care to another within the same patient record, for example, the history and physical posted to the incorrect episode⁴⁰.”

AHIMA suggests that organizations employ specific processes for reporting and correcting such errors found in the EHR that include identifying and monitoring the date of the identified service error³⁹.

All independent clinical scribes are suggested to identify their organization’s specific policies regarding the above-identified types of amendments to the medical record before beginning their Phase II EHR training. Your Scribe Supervisor or facility’s Security Administration or Health Information Management (HIM) personnel can help provide this information.

Review & Assessment

Review

1. Because medical records can be used in a court of law, all interactions with patient health information should be conducted as interactions with legal evidence. Creating, altering, and/or deleting medical health records or patient health information has the potential to constitute tampering with- and/or destroying legal evidence, and should be viewed as such by all clinical scribes.
2. Regulatory standards require that all attempts to access ePHI and all interactions with ePHI be recorded, retained, and periodically reviewed by designated administrative personnel.
3. All healthcare organizations are required to employ policies and procedures for amending medical health records⁴⁰. These policies and procedures should pertain specifically to the following types of amendments:
 - Addendums
 - Corrections
 - Retractions
 - Deletions
 - Late Entries
 - Re-sequencing or Reassignment
4. As a clinical scribe, you are not qualified to instruct your provider on how to care for his or her patients. However, by remaining of aware of “best practices” in medical documentation for preventing legal malpractice, you can ensure that you accurately document all “best practice” measures that your provider engages in.

Assessment

1. Define the following terms and describe how they apply to your role as a clinical scribe:
 - Audit Trail
 - Data Retention
 - Data Availability
 - Data Destruction
 - Record Preservation
2. Read one of the following articles referenced in this chapter and identify 5 tips or takeaways from the article that you can use in your role as a clinical scribe:
 - Dougherty M. How legal is your EHR? Identifying key functions that support a legal record. *Journal of AHIMA / American Health Information Management Association*. 2008;79(2):24-28, 30.
 - McCartney PR. Audit trails and electronic record discovery. *MCN The American journal of maternal child nursing*. 2009;34(1):64.
 - Lugtu T. Toward safer EHR use and documentation. Tips for reducing malpractice risk. *Minnesota medicine*. 2015;98(3):36-37



21

Medicolegal Documentation (II): The Expanded SOOOAAP Note

The Expanded SOOOAAP Note Format for Medico-Legal Documentation

Modules I and II of this manual introduced the **SOAP method of documentation**, in which a medical record may be structured and documented in sections, according to content containing information that is **Subjective**, **Objective**, or relating to the **Assessment** or **Plan**^{41,42}. A newer method of documentation termed the **SOOOAAP or Expanded SOAP method of documentation** has recently been proposed to minimize legal risk associated with medical documentation.

The **SOOOAP method of documentions** segments a medical record into 5 sections containing content that is **Subjective**, **Objective**, or relating to the provider's medical **Opinion**, treatment **Options** discussed with the patient, the provider's medical **Advice**, and the **Agreed-upon Plan**. In this format, the Opinions, Options, Advice, and Agreed Plan sections provide further organization and opportunity for thorough documentation of the provider's medical decision making process that legally supports the quality of care the provider provides to the patient.

The SOOOAAP Note concept was introduced by Dr. Peter Teichman, MD, MPA, in an article titled "Documentation Tips for Reducing Malpractice" published in *Family Practice Management* in 2000⁴³.

- The article is accessible online at: <https://www.aafp.org/fpm/2000/0300/p29.html>.

We recommend that all clinical scribes review this article prior to Phase II and III CSAT training.

We provide a review the article – and SOOOAAP Note charting below.

Subjective: As in the traditional SOAP Note format identified in Module III, the "S" in the SOOOAAP Note format refers to subjective information related to the patient's "new or primary concern"⁴³. This section contains the chief complaint (CC), history of present illness (HPI), and review of systems (ROS). Teichman provides the following additional suggestions for documenting subjective information to reduce legal risks:

- "Use direct patient quotes to highlight main areas of concern, build credibility into the record, and accurately document a patient's competency, affect and attitude⁴³."
- ▶ Teichman provides the example that "if a patient states 'I've been to 20 doctors, and no one can help me,' documenting such a remark communicates his or her attitude⁴³."

- Teichman suggests providers “complete the review of systems with an inquiry such as ‘do you have any other concerns?’”
 - ▶ **When such a question is asked, clinical scribes should document all additional concerns raised by the patient, followed by a statement such as: “patient denies any additional complaints.”**

Objective: As in the SOAP Note format, the Objective portion of the patient’s chart “provides a list of measurable, reproducible data, including citations from laboratory or imaging results⁴³.” Teichman provides the following additional suggestions for obtaining and documenting objective information to reduce legal risks:

- All sensitive examinations such as breast or genital examinations should be performed with a qualified assistant or “chaperone” present in the room, and the presence of the chaperone (including the chaperone initials) should be documented in the examination note⁴³.
- Use “pejorative entries” instead of judgmental or *subjective* descriptors⁴³.
 - ▶ For example, if a patient appears unkempt, the provider is instructed to document “hair oily; scent of body sweat present,” rather than “needs a bath⁴³.”
 - ▶ **As a clinical scribe, your responsibility is to document the dictation of the provider. However, if your provider states after an examination “he needs a bath,” we suggest you confirm whether the provider wants this documented in the patient chart before documenting it.**

Medical Opinion: This section replaces the “Assessment” section of the traditional SOAP note, and reinforces that the provider has communicated his or her medical decision-making process with the patient, including a discussion of the differential diagnoses considered and limitations of the medical diagnosis⁴³. Teichman explains that the legal purpose of this section – in addition to its medical and financial functions – serves to demonstrate the comprehensive thought process involved in the provider’s medical decision-making as well as the quality of care provided to the patient. This section can also serve to demonstrate the provider’s incorporation of patient-centered care. Teichman suggests providers adhere to the following suggestions to reduce legal risks in this portion of the patient encounter, **which should be documented in the patient chart when followed⁴³:**

- Avoid “absolutism” and “false certainties” when discussing the assessment with the patient.

- Discuss the limitations of the assessment as a medical opinion, which may change as new findings develop.
- Discuss medical expectations with the patient regarding different treatment options and diagnoses.
- Discuss the patient's hopes and expectations.
- **In your role as a clinical scribe, we suggest you listen for these points of discussion and document them appropriately in the Assessment or Medical Opinion section of the patient's medical record when they occur.**

Options discussed with the patient: This section supplements the “Plan” section of the traditional SOAP note and supplies evidence of quality patient-centered care and of “informed consent or informed refusal⁴³.” Teichman provides the following suggestions for documenting the options discussed with the patient in this section to reduce legal risks⁴³:

- “Consent and refusal are choices. To choose requires alternatives⁴³.” Therefore, **it is important to document the different treatment options that are discussed with the patient to demonstrate the patient's ability to make an informed decision regarding his or her plan of care.**
- “Throughout the care process, discuss the alternatives, risks and benefits of evaluations and treatments, including a review of likely outcomes if a treatment is withheld or refused, and **document the discussion⁴³.**”
- “In cases where a patient refuses treatment, document his or her ability to understand the repercussions of the refusal.” This may be done by “[**documenting**] in a manner that makes it clear that the patient chose to refuse treatment by using [phrases such as]: ‘consistent with the patient's informed choice...’” Providers are also encouraged to “welcome and document the patient's continual right to reverse his or her decision and receive a recommended treatment.”
- **As a clinical scribe, you are not responsible for the way in which the provider interacts with the patient or the types of discussions the provider engages in. However, you may assist your provider by documenting the above aspects of the provider's discussion with the patient when they occur.**

Medical Advice: “This section distills the medical options discussed above to the best choice for each health concern and funnels the provider's advice into a coherent statement with supportive reasoning⁴³.” Teichman provides the following suggestions for documenting the medical advice

provided to the patient in this section to reduce legal risks⁴³:

- **“Document your reinforcement of the principle that the physician advises and the patient chooses.”**
- “Eliminate festering misunderstandings by confronting unreasonable expectations. For example, you could document ‘futility of antibiotics in this situation reviewed,’ in a case in which you did not write a prescription that a patient thought necessary for treatment.”
- **“Document your encouragement of health maintenance and wellness [by using such phrases as]: ‘urged smoking cessation and offered assistance’⁴³.”**

Agreed-Upon Plan: This section is similar to the “Plan” section in the traditional SOAP note. However, this section prompts and demonstrates patient-centered care by “synthesizing the physician’s guidance and the patient’s choice into a coherent statement that the patient understands and agrees to follow⁴³.” Teichman provides the following suggestions for documenting the agreed-upon plan in this section to reduce legal risks⁴³:

- “Document goals or expected outcomes and specify a time frame for reaching them.”
 - ▶ “Include interval instructions in case of changes in the patient’s condition. For example, [document in the patient’s summary instructions]: **‘recheck if not better in five days, sooner if worse’⁴³.”**
- “Anticipate possible serious adverse outcomes, teach your patients to notify you if they occur and document that you’ve done so⁴³.”
 - ▶ Providers are encouraged to discuss with the patient and document statements such as **“Patient informed of our practice’s 24-hour, 365-day access policy and knows to call any time if an emergency arises.”**
- Discuss and document the known common and severe side effects of any medications or alternative therapies prescribed to the patient.
- Discuss and document the use of “patient-prescribed treatments” with phrases such as **“Communicated that risks and benefits of self-selected treatments not wholly known⁴³.”**
- When a plan is discussed with the patient, providers are encouraged to confirm patient understanding and agreement with the plan, which should be documented in the medical record using a statement such as **“Patient understands and is in agreement with this plan⁴³.”**

- “Document follow-up arrangements with **“Patient agrees to follow up⁴³”** or **“Patient states he will keep appointment⁴³”**.”



SuperScribe Tip:

As a clinical scribe, you are not responsible for the care that your provider renders to his or her patients. However, by remaining informed of the best practice suggestions provided above, you can document your provider’s care more accurately and thoroughly.

Review & Assessment

Recommended Resources

1. Teichman, P. **Documentation Tips for Reducing Malpractice**. *Family Practice Management*. 2000; 7(3):29-33⁴³.
 - <https://www.aafp.org/fpm/2000/0300/p29.html>
 - Introduces Expanded SOOOAAP Note Format for Medico-Legal Documentation
 - Peter Teichman, MD, MPA

Review

1. The **SOOOAAP Note** method of documentation has been proposed to minimize legal risk associated with medical documentation and includes the following sections⁸:
 - Subjective Information
 - Objective Information
 - Medical Opinion
 - Options Discussed with the Patient
 - Medical Advice
 - Agreed-Upon Plan
2. As a clinical scribe, you are not qualified to instruct your provider on how to care for his or her patients. However, by remaining of aware of “best practices” in medical documentation for preventing legal malpractice, you can ensure that you accurately document all “best practice” measures that your provider engages in.

Assessment

1. Read Dr. Teichman's article on SOOOAAP Note Documentation.
 - This can be accessed online at: <https://www.aafp.org/fpm/2000/0300/p29.html>
2. Identify 5 suggestions in the article that you can apply to your medical documentation as a clinical scribe.

A stethoscope with a black tube and silver chest piece is coiled on a light blue background. A wooden gavel with a dark brown handle and head is positioned diagonally across the stethoscope. The gavel's head is resting on the stethoscope's tubing. The background is a solid light blue color with faint, repeating watermarks of a camera icon and the text '123RF'.

Malpractice Prevention

Fraud and False Claims Acts

Fraud is defined as “a deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage⁴⁴.” In the health care industry, fraud has been identified as a growing trend, and enforcement activities are appropriately increasing⁴⁵⁻⁴⁹.

In Module III, we addressed that all health care goods or services must be provided out of **medical necessity** (see **ScribeSense Box on Medical Necessity** below)⁴⁻⁷. As such, all information in the medical record must reflect such medical necessity. For example: a provider may not legally order an expensive MRI study for a patient with a broken finger unless the study can be proven medically necessary. In most cases, an MRI is not medically necessary for the treatment of a broken finger. By coding and billing for this expensive item, the physician would be requesting payment for services that were not medically necessary; this would be similar to the analogy provided earlier of a restaurant providing a customer with a piece of cake that was not ordered, then charging the customer for the order.

All claims for payment rendered to Medicare or Medicaid patients are processed through CMS (or the state equivalent), which is a federally run agency. The **False Claims Act** is a federal law that prohibits any person from knowingly submitting any false claim for payment to the U.S. government⁵⁰. This act applies to any medical claim for goods or services that are either: not medically necessary, or did not occur. Both scenarios fall under the definition of fraud.

The cases below emphasize the importance of understanding and avoiding accusations of medical fraud or false claims in your documentation as a clinical scribe:

- In 2015 the Baptist Health System agreed to a \$2.5 million dollar settlement against allegations that several neurologists were purposefully misdiagnosing patients in order to submit false medical claims to CMS for medically unnecessary procedures and drugs⁴⁹.
- NextCare, a nationwide Urgent Care provider, recently agreed to pay a \$10 million dollar settlement after allegations of “up-coding” their charts by providing tests that were not medically necessary and then coding their charts accordingly⁴⁷.
- In Maryland, an orthopedic practice agreed to a \$2.5 million settlement after allegations of billing for patient visits that never occurred and inappropriately coding x-ray findings to receive higher reimbursement funds⁵¹.

As these cases suggest, coding for services rendered to a patient at a higher code than medically necessary constitutes fraud and is penalized in accordance with the False Claims Act⁵⁰. At all times, the information within a medical record must support the level of service provided to the patient. Violators of the false claims act face treble damages (triple the amount of governmental damages), and jail time if found to be criminally liable for fraud^{50,52,53}.

ScribeSense: Medical Necessity

Medical Necessity is a legal doctrine used primarily to regulate medical service claims made by providers to payers such as patients and insurance companies¹.

The concept of “**Medical Necessity**” was first indoctrinated under the Social Security Act in 1935 which dictated Medicare compensation for all medical items and services deemed “**reasonable and necessary for the diagnosis or treatment of illness or injury**, or to improve the functioning of a malformed body member⁴⁻⁷.”

Although different payers use different criteria to define medical necessity, most definitions require services to be **reasonable, necessary, and appropriate**, based on evidence-based clinical care standards¹. In all cases, **medical necessity must be clearly documented**.

- Medicare has several additional policies that describe **documentation requirements for demonstrating medical necessity**, which include National Coverage Determinations (NCDs) and Local Coverage Determinations (LCDs)^{12,13}.
- Evaluation and Management (E/M) Service guidelines require that **for each service billed, the specific sign, symptom, or patient complaint that makes the service reasonable and necessary must be clearly documented** and medical documentation must support the overall level of service provided to a patient and reported to a payer⁷.
- In general: **all medical services provided and billed must meet medical necessity requirements**, as governed by statutory-, regulatory-, manual-, and NCD/LCD policies⁷.

Reducing Legal Risk in Documentation

As a clinical scribe, your documentation will ultimately provide the information that is reviewed in a medical malpractice proceeding. Understanding this, there are several principles that you can apply to your medical documentation that will help **reduce the legal risk** for unjust conviction of malpractice for your provider. These principles and practices – addressed below – will help you avoid common

legal pitfalls pertaining to medical record documentation.



SuperScribe Tip#1: “If It Was Not Documented, It Did Not Occur”

Documentation connotes existence in the medico-legal world. **Malpractice lawsuits most commonly succeed because of poor, incomplete, inaccurate, or unclear medical documentation**⁵⁴. A well-documented medical record should read like a narrative; any individual should be able to read through a well-written medical record and visualize the events that occurred during a patient encounter in chronological sequence.

The medical record should clearly narrate the provider’s thought process regarding:

Medical decision-making

The timing of each examination

The medical necessity for all services rendered, including:

Physical Examination

All diagnostic studies and procedures

Consultations

Counseling

Patient education

Provider interpretation of all diagnostic studies

Conversations that commence with the patient

The outcome of the patient’s treatment and care

A well-documented medical record leaves no room for questioning or interpretation; all thought and care processes are accurately, clearly, and thoroughly documented. **If a piece of information is not included in the medical record, one may legally assume that piece of information was not documented because it did not occur.** This becomes critically important when considering the ability of a medical record to serve as a business document that supports payment claims. If a provider bills a patient for a service that is not properly documented in the patient's medical record, the provider could be sued for malpractice. Proper documentation must convey that the service:

- Was actually performed
 - ▶ Legally, if a service was not documented, it was not performed, and billing for it can constitute malpractice
- Was rendered by a qualified professional in compliance with applicable regulatory standards
 - ▶ Legally, if a service was not performed according to regulatory standards (including – but not limited to – those imposed by the American Medical Association, CMS, The Joint Commission, and the healthcare provider- or organization's policies), then the provider of the service may be at risk for malpractice – in performing- and billing for the service. This is also true for services that are *performed* according to regulatory standards but without documented evidence of regulatory compliance.
- Was **medically necessary**
 - ▶ Legally, providing a service that is not medically necessary can constitute malpractice, especially in such cases where the provider bills for the service. If the medical necessity of a service is not documented it may not be valid legally.
- Was performed with the informed consent of the recipient
 - ▶ Performing a service without a patient's informed consent violates patient rights. If informed consent is not documented, it does not exist legally.



SuperScribe Tip #2: Document with Accuracy – Check and Re-Check!

In 2014, a major medical professional liability company (CRICO, www.rmfm.harvard.edu) conducted an evaluation of 147 medical malpractice claims⁵⁴⁻⁵⁶. In the study, incorrect information entered into the EHR was found to be the primary contributor of medical malpractice claims involving electronic health record documentation (contributing to 20% of cases)⁵⁴.

In the study, incorrect **information** was found to occur from⁵⁴:

- Faulty data entry
 - ▶ For example, if a patient's height is recorded in cm rather than in inches, which can distort the patient's BMI⁵⁴
- Unexpected conversion
 - ▶ In which the computer auto-converts accurately entered data without user notice, "for example, 2.5 changes to 25, which becomes a medication error when a clinician acts on the higher number⁵⁴."
- Wrong file or field
 - ▶ In which a user accidentally enters information into the wrong file, field, or area of the electronic health record. This can pertain to one patient's information being entered into another patient's record, or one portion of a patient's record being entered into the wrong field, such as if a patient's medication order is entered into the patient's medication history or vice versa.
- Repeated errors
 - ▶ In which mistakes in a patient record persist without being discovered and appropriately corrected.

In the same study, the total entity of factors found to contribute to medical malpractice claims involving electronic health record documentation included⁵⁴:

1. Incorrect information entered into the EHR (accounting for 20% of cases)
2. EHR conversion issues (accounting for 16% of cases)

3. EHR System Failures, including:
 - a. Electronic routing of data (12% of claims)
 - b. Inability to access data (10% of claims)
4. Pre-populating or copy/pasting information into a medical record (10% of cases)
5. EHR System Design's failure to meet medical documentation needs (9% of cases)
6. Poor/insufficient EHR user training or education (7%)
7. Lack of EHR integration/incompatible systems (7%)
8. EHR-related user error other than data entry (7%)

In your role as a clinical scribe, it is critically important that you enter information precisely and accurately into the medical record. Before submitting each record to your provider for review, review the record yourself for accuracy in the following areas:

- Data entry, including accurate units
- Field entry
 - ▶ Ensure that all data is accurately entered into the correct patient chart, and into the correct field within each patient's chart
- Currency
 - ▶ Ensure that all data that already exists in a medical record is accurate and up to date, as corroborated by the provider and patient.



SuperScribe Tip #3: Document Medically Necessary Information

In accordance with the Health Insurance Portability and Accountability Act's (HIPAA) **Privacy Act** and its stipulation for **medical necessity**²⁹, the medical record should not contain any information that is not pertinent to a patient's health or care.

As a scribe, it is important to provide complete documentation of all events that occur during a patient's encounter with a provider. It is not important to include information that is not relevant or necessary to understanding the patient's care. An attorney or non-medical individual may assume (or make a case for) non-relevant information to hold medical, financial, or legal significance that it does not truly hold. In this way, an attorney may discredit a provider's integrity, care, services, or competency based on non-ancillary information documented in a patient's medical record without necessity.

For example, if a work shift is short-staffed for the evening, or if a fire drill occurs in the building during the time in which a provider is providing care to a patient this information should not necessarily influence the quality of care provided to the patient. This being the case, this information should not be documented in the patient's medical record *unless it does directly relate to the patient's care in a way that requires its documentation*. **All information documented in a patient's medical record must have a medically necessary purpose for documentation and inclusion.**



SuperScribe Tip #4: Document Objectively

All descriptors within the medical record should be objective and strictly factual in nature. Inflammatory language, emotional terminology, exaggerations, and opinions (excluding those of the provider related to medical decision making) do not belong in the medical record and should be avoided in medical documentation. **As a clinical scribe, it is your duty to refrain from assigning blame or making assumptions of any kind in your documentation.**

The following examples identify subjective language that should be avoided in medical documentation; these are followed by acceptable objective options for documentation.

1. “The patient is mentally ill and rambling names of Star Trek characters.”
 - “The patient presents alert, but referencing Star Trek characters throughout the history.”
2. “The patient presents with black eye and wrist bruises from domestic abuse.”
 - “The patient presents with R eye hematoma, various contusions to bilateral wrists.”
3. “Patient smells, appears homeless and un-showered for months.”
 - “Patient appears unkempt and malodorous, with oily hair, scent of body sweat noted⁴³.”

Document each medical record you prepare as though it will be read by a jury in a court of law. Objective descriptions prevent the appearance of bias or negative attitude towards the patient.



SuperScribe Tip #5: Document Precisely

Objective documentation is important for a clinical scribe; **precise documentation** is equally important. Vague descriptions should be avoided; documentation should not leave room for interpretation or misinterpretation. Below, examples of vague language that should be avoided are outlined, followed by acceptable more precise options for documentation.

The following examples identify subjective language that should be avoided in medical documentation; these are followed by acceptable objective options for documentation.

1. “The patient has reportedly lost a large amount of blood.”
 - “Approximately 500 cc blood loss reported.”
2. “The patient has had heavy periods and is concerned for blood loss.”
 - “The patient reports changing- or bleeding through one “heavy” tampon every hour for the past 2 days.”
3. “The patient reports experiencing head pain for a long time.”
 - “Patient reports 7/10 head pain for the past 7 hours without relief from Ibuprofen.”

Document each medical record you prepare as though it will be read by a jury in a court of law. Objective descriptions prevent the appearance of bias or negative attitude towards the patient.



SuperScribe Tip #6: Document with Grammatical Accuracy

Ensure use of correct grammar and spelling by reviewing your documentation. Confirm the correct spelling on words that are difficult to spell or pronounce. In particular, confirm your spelling for specific terms such as medications, in which two medications may have similar-sounding names but very different functions. Document as if a legal jury will review your documentation; remain mindful of how a jury may respond to documentation riddled with spelling and grammatical errors.

As a clinical scribe, you have been tasked with the responsibility of providing documentation services on the behalf of your provider. The errors that you add into a chart may be used to create a reflection of your provider's medical competency or to build a case against it.

For example, if a medical document is riddled with spelling and grammatical errors, a jury may be inclined to view the provider – who neglects his or her documentation – as equally negligent or incompetent in providing quality patient care. A plaintiff's attorney may certainly use spelling and grammatical errors to suggest such a claim, discrediting a provider's competency by emphasizing seemingly small errors such as spelling or grammatical mistakes overlooked in the provider's documentation.



SuperScribe Tip #7: Document Timing in a Timely Manner

Providers favor clinical scribe services for the timely – real-time – documentation such services provide. Real-time documentation eliminates the need for a provider to recall and relay an entire physical examination or conversation after it has occurred. “**Recall and relay**” documentation styles are inefficient and inaccurate; a provider may forget to relay or document a specific finding on exam, or may recall a specific finding inaccurately.

Completing a medical record in a timely fashion is an important aspect of patient care that enables rapid communication among many providers. Timely documentation also serves medico-legal functions: timely documentation helps increase documentation accuracy, and helps a facility meet **Meaningful Use and Quality Payment Program criteria “24-hour documentation”²³**. Similarly, including “**time stamps**” – or times associated with various procedures or services provided during a patient’s encounter – can help increase accuracy and specificity of documentation, and can further help a facility support its commitment to meeting and maintaining TJC and **Core Measure standards**.

Documenting the specific times at which various patient care services are provided also provides a more complete chronological narrative of a patient’s encounter that may be useful in the event of a medical malpractice lawsuit.



SuperScribe Tip #8: Document Consistently

All documentation should be conducted in the same format, utilizing only universally accepted abbreviations. Use of shorthand documentation or personal abbreviations outside of those identified in this manual as appropriate for use in medical documentation should be avoided. Consistent compliance with conventional documentation standards helps to avoid later confusion regarding the meanings or implications of any abbreviations or shorthand documentation used in the medical record.

Review & Assessment

Recommended Resources

1. Ruder DB. Malpractice Claims Analysis Confirms Risks in EHRs. *Journal of medical practice management*. 2010;26(1):21-24⁵⁴
 - <https://www.psqh.com/analysis/malpractice-claims-analysis-confirms-risks-in-ehrs/>
 - Overview of CRICO's **Comparative Benchmarking System (CBA)**
 - **CRICO:** Patient safety and medical malpractice insurer that “provides claims management, litigation, and education services to its member owners⁵⁴”
 - **CRICO member owners:** “Over 12,000 physicians, 22 hospitals, and 100,000 nurses, technicians, and other employees of Harvard-affiliated organizations⁵⁴.”
 - CRICO collected large comparative database of claims information from Harvard affiliates and CRICO Strategies partners around the country over the past 30 yrs.
 - **> 275,000 open and closed malpractice cases** from > 500 hospitals and 125,000 physicians over the past 30 years.
 - **CBS:** Taxonomy developed to analyze malpractice claims in CRICO database
 - 2015: CBS expanded to capture **EHR-related problems** that contribute to pt harm
 - **EHR found to be contributing factor in 147 of 275,000 malpractice cases** filed within CRICO database within the past 30 years
 - Reviews Top 9 EHR issues identified in the 147 claims in which EHR-related problems contributed to patient harm
 - Used to “guide hospitals, physicians, and other providers it serves toward addressing vulnerabilities in their systems⁵⁴.”

Review

1. The **False Claims Act** is a federal law that prohibits any person from knowingly submitting a false claim for payment to the U.S. government. This includes any claim for services rendered to a Medicare or Medicaid beneficiary that is false or contains services that are not deemed **medically necessary**.

2. The following documentation practices will help to minimize legal risk with regard to medical documentation:
 - Remembering the mantra: “If an action is not documented it has not occurred.”
 - Document with accuracy: check and re-check.
 - Avoid unnecessary detail.
 - Document precisely.
 - Document objectively.
 - Document with meticulous grammatical accuracy.
 - Document in a timely fashion, and record timing of events.
 - Document consistently.

Assessment

1. Name three tips that you will utilize to ensure your documentation is as thorough and accurate as possible.
2. In 2000, John Davenport, MD, JD published an article in *Family Practice Management* on “Documenting High-Risk Cases to Avoid Malpractice Liability⁹.”
 - a. Access the article online at: <https://www.aafp.org/fpm/2000/1000/p33.html#>
 - b. What are the five clinical conditions that are associated with the highest risk of malpractice suits for family physicians?
 - c. What are the most common causes or types of malpractice lawsuits that occur for each of these five conditions?
 - d. Identify two ways that you can help reduce risk for malpractice in your documentation as a medical scribe for each of these five conditions.

References:

1. contributors W. Medical necessity. 2018; Page Version ID: 853119957:https://en.wikipedia.org/w/index.php?title=Medical_necessity&oldid=853119957. Accessed Feb 21, 2019, 2019.
2. DHHS USDoHaHS. 45 CFR 160.103 - Definitions. In: DHHS USDoHaHS, ed. Vol Title 45, Vol 1. <http://www.govinfo.gov/> Government Publishing Office.
3. Vimalachandran P, Wang H, Y. Z. Securing Electronic Medical Record and Electronic Health Record Systems Through an Improved Access Control. *Health Information Science HIS 2015 Lecture Notes in Computer Science*. 2015;9085:17-30.
4. SSASSA. The Social Security Act of 1935. *Legislative History* <https://www.ssa.gov/history/35act.html>. Accessed Feb 6, 2019, 2019.
5. Medicare Announces Draft Guidance for National Coverage Determinations with Evidence Development [press release]. cms.gov: Centers for Medicare and Medicaid Services 2005.
6. AAFS AAFP. Coding for Evaluation and Management Services. *Payment for Physicians* 2019; <https://www.aafp.org/practice-management/payment/coding/evaluation-management.html>. Accessed Feb 4, 2019, 2019.
7. (CMS) CfMMS, (MLN) MLN, (DHHS) USDoHaHS. Evaluation and Management Services Guide. In: Network DoHaHSCfMMSML, ed. Vol ICN: 006764. <http://www.cms.gov/> Center for Medicare & Medicaid Services (CMS); 2017.
8. Evans RS. Electronic Health Records: Then, Now, and in the Future. *Yearb Med Inform*. 2016;Suppl 1:S48-61.
9. Ventres W, Kooienga S, Vuckovic N, Marlin R, Nygren P, Stewart V. Physicians, patients, and the electronic health record: an ethnographic analysis. *Annals of family medicine*. 2006;4(2):124-131.
10. OCR OoCR. OCR Summary of the HIPAA Privacy Rule. In: Rights USDoHaHS OoC, ed. <http://www.hhs.gov/> U.S. Department of Health and Human Services; 2003:23.
11. OCR OoCR. Summary of the HIPAA Privacy Rule. 2013; <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html?language=en>. Accessed Jan 23, 2019, 2019.
12. CMS CfMMS. National Coverage Determinations (NCDs) Alphabetical Index. *Indexes* 2019; <https://www.cms.gov/medicare-coverage-database/indexes/ncd-alphabetical-index.aspx>. Accessed Feb 6, 2019, 2019.

13. CMS CfMMS. Local Coverage Determinations (LCDs) by State Index. *Indexes* <https://www.cms.gov/medicare-coverage-database/indexes/lcd-state-index.aspx>. Accessed Feb 6, 2019, 2019.
14. DHHS USDoHaHS. 45 CFR 164.501 - Definitions. In: Services USDoHaH, ed. Vol Title 45 Code of Federal Regulations, Subtitle A, Subchapter C, Part 164, Subart E, Section 164.501. <http://www.govinfo.gov/> Government Publishing Office; 2004.
15. DHHS USDoHaHS. 45 CFR § 164.502 Uses and disclosures of protected health information: general rules. In: Services USDoHaH, ed. Vol Title 45. Chapter A. Subhchapter C. <http://www.govinfo.gov/> Government Publishing Office.
16. DHHS USDoHaHS. Security Standards: Administrative Safeguards. In: U.S. Department of Labor WaHD, ed. Vol 2. <http://www.hhs.gov/> U.S. Department of Health and Human Services; 2007.
17. DHHS USDoHaHS. Security Standards: Physical Safeguards. In: Services USDoHaH, ed. Vol 2. <http://www.hhs.gov/> U.S. Department of Health and Human Services; Centers for Medicare & Medicaid Services; 2007.
18. DHHS USDoHaHS. Security Standards: Technical Safeguards. In: Services USDoHaH, ed. Vol 2. <http://www.hhs.gov/> U.S. Department of Health and Human Services; Centers for Medicare and Medicaid Services; 2007.
19. DHHS USDoHaHS. Security Standards: Organizational, Policies and Procedures and Documentation Requirements. In: Services USDoHaH, ed. Vol 2. <http://www.hhs.gov/> U.S. Department of Health and Human Services; Centers for Medicare & Medicaid Services; 2007.
20. OCR OoCR. HITECH Act Enforcement Interim Final Rule. *HIPAA For Professionals* 2017; <https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html>. Accessed Jan 21, 2019, 2019.
21. DHHS USDoHaHS. HITECH Act Enforcement Interim Final Rule. 2017; <https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html>. Accessed Jan 24, 2019, 2019.
22. Institute of Medicine Committee on Data Standards for Patient S. *Key Capabilities of an Electronic Health Record System: Letter Report*. Washington (DC): National Academies Press (US); Copyright 2003 by the National Academy of Sciences. All rights reserved.; 2003.

23. CDC CfDcAP. Meaningful Use. 2017; <https://www.cdc.gov/ehrmeaningfuluse/introduction.html>. Accessed Jan 20, 2019, 2019.
24. Health Information Technology for Economic and Clinical Health Act of 2009. Enacted in the American Recovery and Reinvestment Act of 2009, Title XIII, Pub.L. 111-5, 42 USC 201 Parts 1 - 2. . In: General. USDoHaHSOotI, ed. <http://www.hhs.gov/> U.S. Department of Health and Human Services; 2009.
25. DHHS USDoHaHS. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules In: Services USDoHaH, ed. Vol 78. Fedderal Register: Federal Register; 2013:5566-5702.
26. OCR OoCR, DHHS USDoHaHS. Breach Notification Rule. *HIPAA For Professionals* 2013; <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>. Accessed Feb 17, 2019, 2019.
27. DHHS USDoHaHS. HIPAA Administrative Simplification: Enforcement. In: Services USDoHaH, ed. Vol 74. 45 CFR Part 160; RIN 0991-AB55 ed. Federal Register: Federal Register; 2009:56123-56131.
28. OCR OoCR. The HIPAA Enforcement Rule. 2017; <https://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html?language=en>. Accessed Jan 23, 2019, 2019.
29. DHHS USDoHaHS. 42 CFR § 482.24 - Condition of participation: Medical record services. In: Services USDoHaHSCfMM, ed. <http://www.govinfo.gov/> Government Publishing Office; 2011.
30. DHHS USDoHaHS. 42 CFR § 485.721 - Condition of participation: Clinical records. In: Services USDoHaHSCfMM, ed. <http://www.govinfo.gov/> Government Publishing Office; 1996.
31. U.S. Department of Health and Human Services; Office of the Inspector General. Levinson DRE. 42. U.S.C. 1320a-7a. Civil monetary penalties. Title 42. The Public Health and Welfare > Chapter 7. Social Security > Subchapter XI. General Provisions, Peer Review, and Administrative Simplification > Part A. General Provisions > Section 1320a-7a. Civil Monetary Penalties. In: Services USDoHaH, ed. <http://www.law.cornell.edu/> U.S. Department of Health and Human Services; Reproduced by Cornell Law School; 1935.

32. McKenna SR, Fose RV. The Medical Record and its Role in Litigation. <http://www.hcca-info.org/> Health Care Compliance Association; 2018.
33. OCR OoCR. Minimum Necessary Requirement. 2013; <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html>. Accessed Jan 24, 2019, 2019.
34. OCR OoCR. Minimum Necessary. In: Services USDoHaH, ed. Vol [45 CFR 164.502(b), 164.514(d)] <http://www.hhs.gov/> U.S. Department of Health and Human Services; 2003.
35. Bartschat W, Blevins A, Burnette L, et al. The legal process and electronic health records. *Journal of AHIMA / American Health Information Management Association*. 2005;76(9):96a-96d.
36. Dougherty M. How legal is your EHR? Identifying key functions that support a legal record. *Journal of AHIMA / American Health Information Management Association*. 2008;79(2):24-28, 30.
37. McCartney PR. Audit trails and electronic record discovery. *MCN The American journal of maternal child nursing*. 2009;34(1):64.
38. Lugtu T. Toward safer EHR use and documentation. Tips for reducing malpractice risk. *Minnesota medicine*. 2015;98(3):36-37.
39. Sheber S. New Toolkit Provides Guidelines for EHR Amendments. *Journal of AHIMA / American Health Information Management Association*. 2012. <https://journal.ahima.org/2012/08/29/new-toolkit-provides-guidelines-for-ehr-amendments/>. Accessed Feb 15, 2019.
40. Medical Records: Documentation of Patient Care in the Legal Health Record: From a Risk Management Perspective. *Practice Tips Online Library* <https://www.medicalmutual.com/risk/practice-tips/tip/medical-records-documentation-of-patient-care-in-the-legal-health-record/74>. Accessed Feb 18, 2019, 2019.
41. Lew V, Ghassemzadeh S. SOAP Notes. *StatPearls*. Treasure Island (FL): StatPearls Publishing LLC.; 2018.
42. Pearce PF, Ferguson LA, George GS, Langford CA. The essential SOAP note in an EHR age. *The Nurse practitioner*. 2016;41(2):29-36.
43. Teichman PG. Documentation tips for reducing malpractice risk. *Family practice management*. 2000;7(3):29-33.
44. Dictionary.com. 2019. Accessed Feb 21, 2019, 2019.

45. Health Care Programs: Fraud and Abuse; Revisions to the Office of Inspector General's Exclusion Authorities. Final rule. *Federal register*. 2017;82(8):4100-4118.
46. Medicare and State Health Care Programs: Fraud and Abuse; Revisions to the Office of Inspector General's Civil Monetary Penalty Rules. Final rule. *Federal register*. 2016;81(235):88334-88365.
47. DHHS USDoHaHS, DOJ USDoJ. Annual Report of the Attorney General and the Secretary Detailing Expenditures and Revenues Under the Health Care Fraud and Abuse Control Program for Fiscal Year 2012. In: Services USDoHaH, Justice Do, eds. <http://www.justice.gov/> U.S. Department of Health and Human Services; 2013.
48. Joudaki H, Rashidian A, Minaei-Bidgoli B, et al. Using data mining to detect health care fraud and abuse: a review of literature. *Global journal of health science*. 2014;7(1):194-202.
49. OIG OoIG, DHHS USDoHaHS. Corporate Integrity Agreement Between the Office of Inspector General of the Department of Health and Human Services and Baptist Health. In: General USDoHaHS OoIG, ed. <https://oig.hhs.gov/> U.S. Department of Health and Human Services; Office of the Inspector General; 2015.
50. 31 U.S.C. §§ 3729 - 3733, The False Claims Act. <https://www.govinfo.gov/> Government Publishing Office; 1863.
51. DVA DoVAaHaUDaIAAfFY. Hearings before a Subcommittee of the Committee on Appropriations United States Senate. In: 2002 DoVAaHaUDaIAAfFY, ed. Vol S. Hrg. 107-442. 107th Congress , 1st Session on H.R. 2620/S. 1216. <http://www.govinfo.gov/> Government Printing Office; 2002.
52. Cassidy MA, Horgan JM. Deputy Attorney General issues guidance for enforcement of False Claims Act. *Health care law monthly*. 1998:28-34.
53. Vogel RL. The false claims act and its impact on medical practices. *The Journal of medical practice management : MPM*. 2010;26(1):21-24.
54. Ruder DB. Malpractice Claims Analysis Confirms Risks in EHRs. *Patient Safety & Quality Healthcare (PSQH)*. 2014. <https://www.psqh.com/analysis/malpractice-claims-analysis-confirms-risks-in-ehrs/>. Accessed Feb 15 ,2019.
55. Sato L, Augello TA. Better, Safer Care: Imagining a Medical Record of the Future. *CRICO*. 2012. <https://www.rmfi.harvard.edu/clinician-resources/podcast/2012/emr-of-the-future>. Accessed Feb 20, 2019.

56. CRICO Challenges EMR Complacency [press release]. Cambridge, MA; <http://www.rm.harvard.edu/> CRICO, Feb 6, 2013 2013.
57. Davenport J. Documenting High-Risk Cases to Avoid Malpractice Liability. *Family practice management*. 2000;7(9):33-36.