



PATIENT SAFETY

Interactive Guide for Electronic Medical Records

A supplement to the
Interactive Guide for Office Practices.

AS THE LARGEST NATIONAL INSURER OF PHYSICIAN AND SURGEON MEDICAL LIABILITY,
WE TAKE PRIDE IN DEVELOPING INNOVATIVE PROGRAMS THAT HELP HEALTH CARE
PROFESSIONALS IDENTIFY AREAS OF RISK AND IMPROVE PATIENT SAFETY.

AS PART OF THIS INITIATIVE, WE ARE PLEASED TO PRESENT OUR PATIENT SAFETY
INTERACTIVE GUIDE. THIS INNOVATIVE TOOL WILL HELP YOU AND YOUR OFFICE STAFF
EVALUATE AREAS OF RISK WITHIN YOUR PRACTICE. IT'S ALL PART OF OUR EFFORT TO
WORK TOGETHER TO ADVANCE THE PRACTICE OF GOOD MEDICINE.

How to Use This Interactive Guide for Electronic Medical Records

This interactive guide is not a test. It is a tool designed to help you uncover areas in your practice that could create liability risks or decrease patient safety.

There is no scoring system. The options for responding to statements are **Always/Yes**, **Sometimes**, **Never/No**, and **N/A**. The ideal response to every statement is **Always/Yes** or **N/A**. Any other response indicates an area of potential malpractice exposure in your practice that should be addressed and resolved.

Respond to the statements as objectively and honestly as you can. The effectiveness of this interactive guide depends on how candid you are.

This tool, a supplement to our general Interactive Guide for Office Practices, focuses on the electronic medical record (EMR) and reflects the risks that are seen in office practices that use the EMR.

You can evaluate your office and key systems as a whole by answering all of the questions or focus only on the sections that are areas of concern.

Effective risk management is a team effort. To gain a range of perspectives, we suggest that the physician, dental surgeon/dentist, office manager, and all staff involved with the EMR complete this tool. Any significant variations in the answers among those using this EMR tool should be discussed and addressed. You can also discuss the results with your regional patient safety/risk manager at The Doctors Company.

Knowledge Center

Our extensive online library of published articles is considered to be the industry's definitive resource on today's most pressing patient safety/risk management and health care policy issues.

We've also compiled a selection of complementary articles that can help you lower your liability risk. To read the articles referenced in this tool, visit www.thedoctors.com/emrinteractive.

Expert Team of Trained Specialists

Our patient safety program is led by an expert team of specialists—trained dental, medical, and patient safety professionals who work tirelessly with members to implement risk management strategies tailored to their specialty and their practice.

Our specialists operate regionally and are available to our members for consultation nationwide. E-mail us at patientsafety@thedoctors.com or call us at (800) 421-2368, extension 1243, and we will connect you with your regional patient safety/risk manager.

If you have an urgent patient safety or claims issue, our specialists are available 24 hours a day, 365 days a year on our nationwide hotline at (800) 421-2368.

This interactive guide is not a standard of care. Any guidelines suggested here are not rules, do not constitute legal advice, and do not ensure a successful outcome. The ultimate decision regarding the appropriateness of any action or treatment must be made by each health care practitioner in light of all circumstances prevailing in the individual situation and in accordance with the laws of the jurisdiction in which the care is rendered.

Electronic Medical Records

Every episode of care should be documented objectively, clearly, and completely. The system used by your organization may be written, electronic, or a combination of both. When the paper records are transitioned to electronic format, additional patient safety/risk issues occur. The following areas highlight the components at risk with electronic record keeping.

Always/
Yes

Sometimes

Never/
No

N/A

PASSWORDS

- | | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 1. There is a strict policy regarding passwords and security. |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 2. Passwords are used only by the individual to whom they are assigned. |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 3. Staff members are not granted access to the physician level of security. |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 4. Staff members have their own level of security clearance based on their job functions. |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 5. Only those employees who are required to use the EMR have access to it. |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 6. If all employees have access to the EMR, it is restricted to viewing information (unless entering or editing information is part of the employee's job function). |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 7. When an employee leaves the practice, his or her password is deleted immediately. |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 8. Passwords are periodically changed. |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 9. Passwords require at least two of the following characteristics: numbers, non-alphanumeric symbols, and upper and lowercase letters. |

SECURITY

- | | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|---|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 10. A written security policy is in place and is included in the office orientation of new personnel. |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 11. The security policy is reviewed with staff periodically and includes a reminder regarding electronic security ("phishing") scams. |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 12. The policy includes how to safely access the EMR through laptops and other remote computers so that the system remains secure. |

Electronic Medical Records

Always/
Yes Sometimes Never/
No N/A

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

SECURITY

13. Computer disks are locked at the close of business every day.
14. The security policy has established a time frame for automatic log-off during periods of inactivity.
15. A firewall is in place.
16. Up-to-date encryption standards and technology (National Institute of Standards and Technology—NIST) protect data.
17. Computer terminals are locked during periods of inactivity and prior to staff leaving the office.

PATIENT ENCOUNTER RECORDS

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

18. Information is entered into the EMR immediately after the patient's visit.
19. If you do not enter notes immediately, you dictate them after the exam for later entry.
20. The date of dictation or date of transcription is included in the record.
21. The author of each entry takes a specific action to verify that the entry is his or hers and is accurate.
22. The author signs the patient encounter entry once it is completed.
23. Once the patient encounter is completed, it is locked in the system and cannot be changed or revised.
24. If information needs to be added or comments made after the entry is locked, the new entry is clearly identified as an addendum with current date, references the date being amended, and includes the reason for the late or corrected entry and an electronic signature.
25. The individual who makes a change or addendum ensures that it is clearly identified in the record.
26. The cut and paste function has been disabled (if the system includes that capability).

Electronic Medical Records

Always/
Yes Sometimes Never/
No N/A

PATIENT ENCOUNTER RECORDS

27. There is a policy that stipulates if, when, and how the copy and paste function may be used.

28. Allergy documentation is displayed consistently and prominently.

29. If there is a medication module, it is activated and used correctly.

30. Review of autopopulated fields is confirmed or corrected at each patient encounter.

31. Alerts, warnings, reminders, and embedded practice guidelines cannot be overridden or disabled.

TEMPLATES

32. EMR templates cannot be repopulated with the same data for each subsequent visit.

33. The system requires the practitioner to manually select “resolved” before a complaint is noted as being “resolved” rather than automatically defaulting to “resolved.”

34. Notes are individualized for each patient encounter, and relevant sections are reviewed to avoid importing incorrect, redundant, or irrelevant information.

35. There is a clear method for knowing that the physician sign-off has occurred at the end of the visit; e.g., the note is signed by the physician.

36. The EMR has an “audit trail” to trace staff entries.

37. Orders or e-mails are reviewed before they are signed off with electronic signatures.

38. The system requires the author to review the entry prior to authenticating it.

39. Clinical personnel are prevented from universally approving a series of orders or e-mails without reading them.

Electronic Medical Records

Always/
Yes Sometimes Never/
No N/A

TEMPLATES

40. If the completion of all fields is not required, “N/A” must be entered.

41. If the system has generic templates, they have been reviewed for relevancy to their specific patient populations.

TRACKING SYSTEMS

42. The EMR has a tracking system to help ensure that patients have completed recommended tests or consultant referrals.

43. The tracking system includes:

a. verification that the patient kept the appointment or completed the test,

b. confirmation of receipt of the report,

c. prompts to call the consultant, imaging center, or lab if a report is not received,

d. verification that the physician has reviewed the report,

e. verification that results were communicated to the patient,

f. arrangements for follow-up if necessary, and

g. documentation of all these steps with dates and electronic signatures.

PAPER AND EXTERNAL CLINICAL DOCUMENTS

44. All paper documents are scanned into the EMR.

45. The scanned documents include paper records used before implementing an EMR, such as diagnostic test results, consultant reports, hospital reports, or records from other physician offices.

46. The process ensures that once scanned, the paper documents are then properly stored or destroyed.

47. If the system has limited memory or scanning capability, the physician reviews the records, summarizes them, and includes that information in the patient’s history within the EMR.

Electronic Medical Records

Always/
Yes Sometimes Never/
No N/A

PAPER AND EXTERNAL CLINICAL DOCUMENTS

48. If a summary is used, the paper records are stored.

49. If the system has the memory and capability, all documents are scanned.

50. If the system memory cannot hold all paper documents, the original paper records are retained in the event copies are needed.

51. There is a policy for capturing patients' previous medical records, and it is consistently followed.

52. There is a policy addressing retention periods for paper records after they are scanned.

53. Images that have been scanned are sampled to ensure quality.

PRESCRIPTIONS

54. If e-prescribing is not used, prescriptions are captured by scanning the paper prescription into the EMR.

55. If the paper prescription is not scanned, the prescription documentation includes the patient's name, dose, quantity, instructions, indications, and refill amount.

56. If sample medications are dispensed, there is documentation of the medication name, dose, quantity, indications, and instructions included in the EMR.

57. If medication "pick lists" are used for e-prescribing, they are structured to reduce or eliminate look-alike drugs from being prescribed.

BACKUP

58. Patient data is backed up to ensure it can be retrieved if a hardware failure or other problem occurs.

59. The backup record is regularly tested to ensure that all appropriate data are being copied and that data restoration is possible.

Electronic Medical Records

Always/
Yes Sometimes Never/
No N/A

BACKUP

60. Testing is done for all types of backups, including in-house creation on a removable hard drive and processes that send the information over the Internet for offsite storage.

61. If the EMR vendor provides offsite backup, you have confirmed that the data is created appropriately.

PRINTED ELECTRONIC RECORDS

62. When printing a complete record, it:

a. shows the electronic signature and date the physician signed the progress note,

b. indicates when entries were made by staff and shows their initials or unique identifier,

c. shows all lab and consult reports with the physician signature and date indicating timely review,

d. shows all medications prescribed, refills authorized, and samples given (if relevant),

e. includes patient consent forms, and

f. includes all patient telephone calls.

63. A staff member is assigned to ensure that a complete record is printed prior to being sent.

64. There is a policy defining which images constitute the official medical record.

65. When scanning a patient's paper records, the print function is tested to make sure it captures everything from the scanned documents.

66. There is a system in place to ensure that written documentation of phone calls or requests for medication refills are scanned into the EMR.

Electronic Medical Records

Always/
Yes Sometimes Never/
No N/A

USE OF EMR IN EXAM ROOMS

- | | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 67. The computer screen is positioned for easy viewing by both physician and patient. |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 68. You talk to the patient first before turning your attention to the computer and reviewing the EMR. |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 69. You make eye contact and use active listening skills while talking with the patient. |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 70. You show the patient information in the EMR that is relevant to his or her treatment. |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 71. All EMR users are able to locate information in the record quickly. |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 72. You are adept at entering information into the EMR while minimizing attention away from the patient. |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 73. A patient satisfaction survey was conducted before and after the EMR was implemented. Responses are reviewed and action is taken as appropriate. |

EMR DOCUMENTATION CORRECTIONS

- | | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|---|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 74. Your vendor has confirmed that your EMR system allows error correction without overwriting the erroneous entry. |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 75. The system has the ability to track corrections or changes once the original entry has been entered or authenticated. |
| | | | | 76. When correcting or making a change to an entry, the: |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | a. original entry is viewable, |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | b. current date and time are entered, |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | c. person making the change is identified, and |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | d. reason for the change or correction is noted. |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 77. If a hard copy is printed from the EMR, it has also been corrected. |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 78. The system offers the ability to suppress viewing errors, but it ensures that flags notify others of any corrections. |

Electronic Medical Records

Always/
Yes Sometimes Never/
No N/A

EMR DOCUMENTATION CORRECTIONS

79. The location of the error points to the correction.

80. There is a policy to ensure that personnel correct and report documentation errors in the record, in a consistent and timely manner.

OTHER ISSUES

81. Staff has received formal education and training on EMR documentation, security, and confidentiality, including HIPAA regulations.

82. Updates and refresher education are provided.

83. There is a policy that defines the legal aspects of the EMR.

84. There is a policy to address documentation when EMR systems are unavailable due to planned or unplanned downtimes.

TIPS

- Doctors are responsible for the information they can reasonably access. Review all available patient information.
- If using e-prescribing, be aware of the patient’s entire inpatient and outpatient medication history. Reconcile any drug interaction alerts that you receive.
- Don’t ignore, override, or disable alerts, warnings, reminders, and embedded practice guidelines.
- Be careful of the copy and paste feature. It doesn’t take the place of thoughtful review and analysis, and it can result in failure to update patient information.
- Be aware that the use of templates may compromise accurate documentation, so make sure your documentation accurately describes the patient’s condition.
- Don’t let the computer become a communication barrier between you and your patient.
- Vendor contracts may attempt to shift medical liability risk from faulty software design onto the physician. Read contracts carefully.
- Remember that all interactions with the EMR are time-tracked and discoverable.
- Know the source of the medication and clinical decision support information provided with your EMR.
- Follow HIPAA regulations related to protecting “individually identifiable health information.”

Additional information at www.thedoctors.com/emrinteractive:

- Electronic Medical Record and Social Media Malpractice Risks
- eRisk Guidelines for Online Communication
- EHR “Meaningful Use” Alert