Decipher the Complexities of the Electronic Medical Record

EDITED BY
Vickie L. Milazzo RN, MSN, JD
NEW YORK TIMES BESTSELLING AUTHOR
THE PIONEER OF LEGAL NURSE CONSULTING
© 2013 Vickie Milazzo Institute, a division of Medical-Legal Consulting Institute, Inc., Houston, Texas.

No part of this work may be reproduced or transmitted in any form or by any means, digital, electronic or mechanical, including photocopying or scanning, or by any information storage or retrieval system without permission in writing from Vickie Milazzo Institute.

DISCLAIMER OF WARRANTIES

THIS ADVANCED CLNC® PRACTICE-BUILDING PROGRAM PROVIDED BY VICKIE MILAZZO INSTITUTE ("INSTITUTE") IS TRANSFERRED AND SOLD TO THE PURCHASER WITHOUT ANY WARRANTIES BY THE INSTITUTE, WRITTEN OR ORAL, EXPRESS OR IMPLIED, INCLUDING WARRANTY OF MERCHANTABILITY, FITNESS FOR PARTICULAR PURPOSE, USE, OR OTHERWISE. SUCH MATERIALS ARE SOLD ON AN "AS IS" BASIS AND THE INSTITUTE ASSUMES NO LIABILITY OR RESPONSIBILITY FOR ANY SUBSEQUENT USE BY PURCHASER.

END-USER LICENSE AGREEMENT

This educational material is copyrighted by Medical-Legal Consulting Institute, Inc./Vickie Milazzo Institute, and is provided to the original licensee under a personal education license. This material may not be transferred, sublicensed, resold, reproduced, copied or otherwise redistributed in whole or in part in any form without prior written permission of the licensor. By opening and continuing to use this material you agree to the terms of such license.
DECIPHER THE COMPLEXITIES OF THE ELECTRONIC MEDICAL RECORD FOR YOUR ATTORNEY-CLIENTS

CONTENTS

I. Introduction ................................................................................................................................. 1

II. Software Uses, Documentation Policies and the Discovery Process ........................................ 2

III. Sources of Documentation ........................................................................................................ 3

IV. Interrogatories and Requests for Production ........................................................................... 5

V. Tampering, Falsifying Records, Omissions and Late Additions ..................................................... 10

VI. EMR Problems .......................................................................................................................... 11

VII. The Role of the Certified Legal Nurse Consultant® in Cases Involving Electronic Medical Records ......................................................................................................................... 12

VIII. Recommended Qualifications for CLNC® Subcontractors for Cases Involving Electronic Medical Records ............................................................................................................................. 12

IX. Resources .................................................................................................................................. 13
DECIPHER THE COMPLEXITIES OF THE ELECTRONIC MEDICAL RECORD FOR YOUR ATTORNEY-CLIENTS

I. INTRODUCTION

A. Electronic Medical Records (EMRs) Are Part of the Electronic Health Record (EHR)
   1. EMRs are a digital version of a paper chart from a hospital or doctor's office.
   2. EHRs are the lifetime health information of a patient through multiple care settings and providers.

B. EMRs Are Complex
   1. Necessitate clear and specific requests during discovery to obtain the results the attorney-client requires.
   2. Require an understanding of health information technology terminology. (Exhibit A)
   3. May require copies of procedures related to EMRs and to the case.
   4. May contain additional clinical information from other clinical settings or facilities through health information exchanges (HIEs).

C. EMRs Are Not Designed or Implemented Exactly the Same
   1. Consider design, stages of implementation, upgrades, etc.
   2. Be aware that software from same vendor is configured differently at different facilities.
   3. May be implemented in one state but used in another and may not meet all state laws.
D. **EMRs Must Meet Regulatory Requirements**

1. May detract from quality patient care.
   a. Penalties up to millions of dollars for not meeting certain regulations can shift focus to documentation rather than appropriate patient care.

2. Regulation examples: Meaningful Use Stage 1 and Readmissions Management

II. **SOFTWARE USES, DOCUMENTATION POLICIES AND THE DISCOVERY PROCESS**

A. **EMR Implementation and Upgrades**

1. When changing from paper to computerized records, parts of the system may be phased in at different times.

2. When changing from one vendor to another, gaps may require interim work arounds.

3. When upgrading software, all major and minor changes must be communicated.

4. All of the above situations require policies to govern documentation and training procedures.
   a. Failure to understand, and competently use healthcare software can impact how clinicians document.

B. **Training**

1. Categories.
   a. Initial.
   b. Downtime.
   c. Ongoing.
   d. Orientation.

2. Types.
   a. End-user classes.
   b. Online.
   c. Videos.
   d. Train the trainer.
C. Accessing the EMR

1. Role-based access.
2. Login and passwords.
3. Timeouts.

D. Discovery Questions

1. Emergency department (ED): During a code there frequently isn't enough time to document in real time. Vitals are written on a paper towel or the bed sheet. Times meds are given are from memory. In the EMR the documentation times are entered, date and time stamped along with the name of the person entering the data.
   a. If there is a scribe designated to document during a code, does that person document in the EMR?
   b. What happened to the documentation on paper?
   c. How long after the code did the charting occur?
      (1) Does the time lapse appear in the EMR?

2. Operating room (OR): A surgical patient has a post-surgical infection. No clear-cut source of contamination is evident. However, in reviewing the OR schedule, a Class IV surgical wound surgery occurred in the same OR just before the plaintiff’s surgery.
   a. What was the time between the two surgeries?
   b. What is the procedure to clean between surgical cases?
   c. What documentation shows the cleaning was done?

3. Nursing home: Charting on night shift for the patient with fluid restriction is incomplete or shows a fluid overload on some nights. The night nurse on several of those occasions is an agency nurse. She denies documenting in the EMR. She states she asked the nurse aide to document I & O.
   a. What is the agency nurse’s login and password?
   b. What is the policy about who can document I & O?
   c. Who is monitoring the fluid restriction on the patient ongoing?

III. SOURCES OF DOCUMENTATION

A. The Patient’s Clinical Information

1. Inpatient records.
2. Physician office records.
3. ED records.
4. Urgent care records.
5. Past medical records.
6. Email and direct project messages.

B. Other Software Sources of Information
1. Pharmacy records.
2. Insurance records.
3. Laboratory information systems.
4. Cardiology information systems.
5. OR information systems.
6. Coding systems.
7. Radiology and picture archival computerized systems (PACS).
8. Physiological monitoring systems.
10. Home health systems.
11. Decision support systems.
12. Patient acuity systems.
13. Case management systems.

C. Outside Sources
1. Health Information Exchanges (HIE).
2. Regional Health Information Organizations (RHIO).
3. Patient-personal health record (PHR) web portals.
4. Provider web portals.
5. Healthcare websites.
6. Mobile devices (facility owned, privately owned).

7. Electronic dashboards
   a. Clinical (i.e. modified early warning systems).
   b. Operational, financial (scorecards).

8. Computerized reports.

IV. INTERROGATORIES AND REQUESTS FOR PRODUCTION

A. Interrogatories Directed to the Defense

1. Please describe the components of physician documentation that were computerized, along with the source application(s) and those components that were paper based at (Facility) __________ from (Date) __________ to (Date) __________.

2. Please describe the components of nursing documentation that are computerized, along with the source application(s) and those components that were paper based at (Facility) __________ from (Date) __________ to (Date) __________.

3. Please describe the process for reviewing department and hospital policies regarding computerized medical records that were in effect at (Facility) __________ from (Date) __________ to (Date) __________.

4. Please describe how software upgrades are communicated to end users at (Facility) __________ from (Date) __________ to (Date) __________.

5. Describe the frequency and types of training given to end users of (Name of system) __________ at (Facility) __________ from (Date) __________ to (Date) __________.

6. Please describe the orientation for new employees using healthcare software (Name of system) __________ at (Facility) __________ from (Date) __________ to (Date) __________.

7. Please describe how competency in using of healthcare software (Name of system) __________ is measured for new employees and on an ongoing basis for current employees at (Facility) __________ from (Date) __________ to (Date) __________.
8. Describe the process for procuring a login and password for (Name of system) _________ at (Facility) _________ from (Date) ____________ to (Date) ____________.

9. Describe how agency nurses are given logins and passwords on weekends and holidays for (Name of system) _________ at (Facility) _________ from (Date) ____________ to (Date) ____________.

10. Describe the use of generic passwords for agency nurses, information clerks, medical records clerks, etc.) for (Name of system) _________ at (Facility) _________ from (Date) ____________ to (Date) ____________.

11. Describe the use of generic passwords for student nurses for (Name of system) _________ at (Facility) _________ from (Date) ____________ to (Date) ____________.

12. Describe the use of generic passwords for medical record clerks for (Name of system) _________ at (Facility) _________ from (Date) ____________ to (Date) ____________.

13. Describe security measures in place to prevent an unauthorized user from accessing (Name of system) _________ at (Facility) _________ from (Date) ____________ to (Date) ____________.

14. Describe the process for entering patient information in the event of an emergency such as a code into (Name of system) _________ at (Facility) _________ from (Date) ____________ to (Date) ____________.

15. Describe the use of scribes if used in entering patient information into (Name of system) _________ at (Facility) _________ from (Date) ____________ to (Date) ____________.

16. Describe what healthcare software systems are audited at (Facility) _________ from (Date) ____________ to (Date) ____________ and the process for determining which data elements are monitored.

17. Please describe the process for updating the computer images across the enterprise at (Facility) _________ from (Date) ____________ to (Date) ____________.

B. Interrogatories Directed to the Plaintiff

1. Please list all the experts you intend to call who are familiar with (Electronic medical record software) _________ used at
(Facility)__________ from (Date) ____________ to (Date) ____________, including:

a. Full name.
b. Address.
c. Telephone number.
d. Level of education
e. Work history for past five years.

2. Please list all witnesses you intend to call who were present during the incident (cardiac arrest, vaginal delivery, etc.) on (Date) ____________ responsible for charting all care delivered to plaintiff from (Time) ____________ to (Time) ____________, including:

a. Full name.
b. Address.
c. Telephone numbers.
d. Title.
e. Level of education.

3. Please describe the standard, policy and/or regulation that have been breached in relation to the plaintiff’s injury.

4. Please describe the details of how the plaintiff’s privacy was violated (phone call, drop-in visit, Facebook).

5. Please describe the plaintiff’s allegations in detail as they pertain to the registered nurse (RN) documenting care in the plaintiff’s room in the ED (conversation at bedside).

6. Please describe how the plaintiff’s spouse gained access to the plaintiff’s personal health record without knowledge of a login and password.

C. Requests for Production Directed to the Defense

1. Please provide a copy of the approved policies related to monitoring and auditing the EMR used at (Facility) ____________ from (Date) ____________ to (Date) ____________.

2. Please provide a copy of the approved policies related to clinical documentation used at (Facility) ____________ from (Date) ____________ to (Date) ____________.

3. Please provide an audit and security record of all entries in the EHR and any other clinical documentation related to (Plaintiff) ____________ at (Facility) ____________ from (Date) ____________ to (Date) ____________ including any data repositories that exist.
4. Please provide the manual, CD and or video training that is provided to the Registered Nurses before using (Name of system) __________.

5. Please provide the manual, CD or video training that is provided to the physician before using (Name of system) __________.

6. Please provide the manual, CD or video training that is provided to the agency nurse before using (Name of system) __________.

7. Please provide a copy of the software upgrade educational material provided to users at (Facility) __________ from (Date) __________ to (Date) __________.

8. Please provide the downtime procedures for (Name of system) __________ for each department at (Facility) __________ from (Date) __________ to (Date) __________.

9. Please provide the backup nursing documentation provided for use by RNs in case of computer downtime greater than one hour at (Facility) __________ from (Date) __________ to (Date) __________.

10. Please provide a copy of the process to obtain medical records greater than three years old at (Facility) __________ from (Date) __________ to (Date) __________.

11. Please provide a copy of the approved policy for password provisioning at (Facility) __________ from (Date) __________ to (Date) __________.

12. Please provide a copy of all privacy and security policies for the information technology department at (Facility) __________ from (Date) __________ to (Date) __________.

13. Please provide a copy of the user enhancement requests to (Software vendor) __________ from departments and individuals at (Facility) __________ from (Date) __________ to (Date) __________ and the reason for each request.

14. Please provide a copy of the project plan for the implementation of (Computer application) __________ at (Facility) __________.

15. Please provide a copy of (Plaintiff) __________’s personal health record in its entirety from the enterprise web portal at (Facility) __________ from (Date) __________ to (Date) __________.
16. Please provide a list of the “bugs,” issues and problems list from the vendor of (Computer application) __________ from (Date) __________ to (Date) __________.

D. Requests for Production Directed to the Plaintiff

1. Please provide all written documents that plaintiff obtained related to the use of (Software program) __________ used at (Facility) __________ from (Date) __________ to (Date) __________.

2. Please produce written report from plaintiff’s subsequent treating physician from (Date) __________ to (Date) __________. Please include:
   a. Any medical record indicating a diagnosis was not properly entered into the EMR at (Facility) __________ from (Date) __________ to (Date) __________, resulting in delay of treatment.
   b. All subsequent care related to inadequate information in the EMR at (Facility) __________ from (Date) __________ to (Date) __________.

3. Please produce any photos or videos taken of plaintiff that demonstrate damages from (Date) __________ to (Date) __________.

4. Please provide any recordings of prehospital communications that demonstrate history of patient prior to arrival at the hospital.
   *(Frequently not passed on or overlooked.)*

5. Please provide audit trails of plaintiff’s EMR from (Date) __________ to (Date) __________ and all late entries and addendums pertaining to said hospital stay and episode of care including legend of abbreviations and acronyms. *(Fraud.)*

6. Please provide a detailed list of what features were audited for (Software program or programs) __________ used at (Facility) __________ from (Date) __________ to (Date) __________.

7. Please provide the computer training records of all employees who documented on the plaintiff’s chart for (Software program) __________ used at (Facility) __________ from (Date) __________ to (Date) __________.

8. Please provide documentation of scheduled and actual downtime for (Software program) __________ used at (Facility) __________ from (Date) __________ to (Date) __________.
9. Please provide a detailed list of any and all generic passwords used by employees responsible for charting all care delivered to plaintiff from (Date) __________ to (Date) __________.

V. TAMPERING, FALSIFYING RECORDS, OMISSIONS AND LATE ADDITIONS

A. Audit Records
   1. May not be used to track all applications.
   2. Many applications and single databases do not have audit capability.
   3. Audit trails may not track all activity within an application.
   4. Staff are the first to learn and use shortcuts.
      a. Ask about use of shortcuts if omissions appear to an issue.

B. Policies
   1. Should be written for how auditing is maintained.
   2. Should include how addendums and late entries are entered.
   3. Should include who has access to computerized records.

C. Passwords
   1. Should be changed according to facility policy.
      a. Any exceptions should be documented in the policy (including IT).
   2. Should never be shared.
   3. No generic passwords should be used.
   4. Employees that quit, are fired or laid off should be prevented from accessing the system based on policy in timely manner and audited.

D. Downtime Procedures
   1. Staff should be educated.
      a. New employees should be trained.
2. All paperwork should be included as part of the patient medical record even if some data is entered into the computer application.  
   a. This may differ based on hospital policy.

E. Access

1. Should be role based to comply with privacy and security standards.

2. Can be tracked through auditing if auditing is turned on for that application.

3. Students, residents, interns, agency nurses and volunteers should be role based with individual access.

4. Electronic signature in an application should be verified by a clinician.  
   a. Some systems sign attending doctor without review.

VI. EMR PROBLEMS

A. A Facility Can Have Different Versions of EMR Software Running

1. How EMR software looks and runs on different browsers (Internet Explorer, Chrome or Mozilla) can affect performance and function.

B. Record Keeping Can Be Poor or Nonexistent for Software Upgrades, Images, Hardware Changes and Locations

C. Issues with EMR Software Are Readily Known by Staff Using It

1. Requests to vendors for changes may exist from facility or other facilities for known problems.

D. Vendors Have Known Bug Lists

1. End users may or may not be aware of those bugs.

2. If an end user feels they did everything they were taught and encounter an unexpected result in the computer application, this may be worth investigating.
3. Performance can be affected by how many people are on the system, bandwidth or amount being audited.
   a. Auditing may be cut back incrementally or completely turned off.

VII. THE ROLE OF THE CERTIFIED LEGAL NURSE CONSULTANT® IN CASES INVOLVING ELECTRONIC MEDICAL RECORDS

A. Can Use Clinical Experience to Track What Should Be on the Patient Record
   1. Ask for appropriate policies governing clinical and IT documentation and procedures.
   2. Interpret documentation policies or lack of to determine where information should be located and what may be missing.
   3. Assist attorney-clients in finding CLNC® consultants with informatics experience.

B. Use Clinical Experience to Track Additional Software Systems That May Contain Relevant Clinical Information
   1. Seek out laboratory, radiology and case management systems.

C. Interpret Audit Trails with an IT Resource or CLNC® Informaticist

D. Suggest Additional Sources of Clinical Information to Support the Case

VIII. RECOMMENDED QUALIFICATIONS FOR CLNC® SUBCONTRACTORS FOR CASES INVOLVING ELECTRONIC MEDICAL RECORDS

A. Experience
   1. A BSN or higher plus a degree in healthcare or nursing informatics or health information management or five or more years equivalent experience.
2. At least 2,000 hours in past three years in nursing informatics and 15 hours minimum of continuing education in nursing informatics in past three years.

B. Certifications Recommended
1. CPHIMSS, RHIT and CHISP.

C. Membership in Professional Organizations
1. HIMSS, AMIA, ANIA and ASHIM.

IX. RESOURCES

A. Professional Organizations
1. American Health Information Management Association (AHIMA).
   ahima.org
2. American Medical Informatics Association (AMIA).
   amia.org
   nursingworld.org
   ania.org
5. American Society of Health Informatics Managers (ASHIM).
   ashim.org
   himss.org

B. Authoritative Textbooks


C. Websites

   [gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf](http://gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf)

2. Health and Human Services (HHS) is responsible for implementation and management of health and human service recovery act programs.
   [hhs.gov](http://hhs.gov)

3. KLAS independently monitors vendor performance through the active participation of thousands of healthcare organizations. KLAS uses a stringent methodology to ensure all data and ratings are accurate, honest and impartial.
   [klasresearch.com](http://klasresearch.com)

4. Office of the National Coordinator for Health Information Technology
   [healthit.gov](http://healthit.gov)

D. Publications

   [journals.lww.com/cinjournal/pages/default.aspx](http://journals.lww.com/cinjournal/pages/default.aspx)

   [healthcareitnews.com](http://healthcareitnews.com)
## Exhibit A
### Glossary

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARRA</td>
<td>American Recovery and Reinvestment Act. (Public Law 111-5). The Health Information Technology for Economic and Clinical Health Act (HITECH) is part of this law.</td>
</tr>
<tr>
<td>Bug</td>
<td>An error or unexpected result in a computer application which makes it behave in an unintended way. In healthcare this could have medical and legal consequences as it can affect patient care.</td>
</tr>
<tr>
<td>Class 1 Medical Device</td>
<td>Food and Drug Administration (FDA) designation which defines requirements for medical devices. There are three classes in the U.S. Note: Some healthcare software can be a Class 1 medical device.</td>
</tr>
<tr>
<td>CDS or CDSS</td>
<td>Clinical decision support or clinical decision support system.</td>
</tr>
<tr>
<td>CPOE</td>
<td>Computerized physician order entry.</td>
</tr>
<tr>
<td>Downtime</td>
<td>When a computer and/or its software application(s) cannot be accessed.</td>
</tr>
<tr>
<td>eMAR</td>
<td>Electronic medication administration record.</td>
</tr>
<tr>
<td>EHR</td>
<td>Electronic health record.</td>
</tr>
<tr>
<td>EMR</td>
<td>Electronic medical record.</td>
</tr>
<tr>
<td>FDA</td>
<td>Food and Drug Administration.</td>
</tr>
<tr>
<td>HIE</td>
<td>Health Information Exchange can be local, regional, state or larger.</td>
</tr>
<tr>
<td>HIT</td>
<td>Health information technology.</td>
</tr>
<tr>
<td>HITECH</td>
<td>Health Information Technology for Economic and Clinical Health Act.</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and communication technology.</td>
</tr>
<tr>
<td>Meaningful Use</td>
<td>Meaningful use sets healthcare goals to improve quality, safety and efficiency of patient care, engage patients and families, improve care coordination, ensure adequate privacy and security for personal health information and improve population and public health.</td>
</tr>
<tr>
<td>Mobile Apps</td>
<td>Applications created to run on handheld devices such as phones or tablets.</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td>PACS</td>
<td>Picture archiving and communication system for medical images.</td>
</tr>
<tr>
<td>PHR</td>
<td>Personal health record.</td>
</tr>
<tr>
<td>Portal</td>
<td>Website where patients and providers can educate, view, create and exchange clinical information securely.</td>
</tr>
<tr>
<td>RHIO</td>
<td>Regional health information organizations.</td>
</tr>
<tr>
<td>SPR</td>
<td>Student patient record. Residents’ application to document clinical information for educational purposes.</td>
</tr>
</tbody>
</table>
Eligible professionals (EPs) and hospitals need to successfully attest to demonstrating meaningful use of certified electronic health records (EHRs) to qualify for an incentive payment through the Medicare EHR Incentive Program administered by the Centers for Medicare and Medicaid Services (CMS). EPs and hospitals that are eligible for the Medicaid EHR Incentive Program do not need to attest to meaningful use in their first year of participation, but must adopt, implement or upgrade to an EHR to receive an incentive payment from their state.

**Summary of Meaningful Use Criteria and Objectives**

In order to meet the meaningful use criteria, EPs and hospitals must adopt certified EHR technology and use it to achieve specific objectives.

EPs and hospitals must become meaningful users of certified EHRs to qualify for incentive payments through the Medicare EHR Incentive Program administered by CMS.

The meaningful use criteria, objectives and measures will evolve in three stages over the next five years:

1. **Stage 1 – 2011-2012.**
   Data capture and sharing.

2. **Stage 2 – 2013.**
   Advance clinical processes.

3. **Stage 3 – 2015.**
   Improved outcomes.
Meaningful Use Criteria

Stage 1
Meaningful Use Criteria Focus

Electronically capturing health Information in a standardized format.
Using that information to track key clinical conditions.
Communicating that information for care coordination processes.
Initiating the reporting of clinical quality measures and public health information.
Using information to engage patients and their families in their care.

Stage 2
Meaningful Use Criteria Focus

More rigorous health information exchange (HIE).
Increased requirements for e-prescribing and incorporating lab results.
Electronic transmission of patient care summaries across multiple settings.
More patient-controlled data.

Stage 3
Meaningful Use Criteria Focus

Improving quality, safety and efficiency, leading to improved health outcomes.
Decision support for national high-priority conditions.
Patient access to self-management tools.
Access to comprehensive patient data through patient-centered HIE.
Improving population health.

Achieving meaningful use during Stage 1 requires meeting both core and menu objectives. All of the core objectives are required. EPs and hospitals may choose which objectives to meet from the meaningful use menu set.

**Meaningful Use Criteria for EPs**
1. 15 core objectives.
2. Five out of ten from menu set objectives.
3. Six total clinical quality measures.
   a. Three core or alternate core.
   b. Three out of 38 from additional set.
Meaningful Use Criteria for Eligible Hospitals/CAHs
1. 14 core objectives.
2. Five out of ten from menu set objectives.
3. 15 clinical quality measures.

Clinical Quality Measures
As part of meeting one of the meaningful use core measures, EPs and eligible hospitals must report on clinical quality measures in order to successfully attest to meaningful use and receive an incentive payment. For information on clinical quality measures, including how to report on them from an EHR, visit the CMS Quality Measures webpage.

Health IT.gov. Meaningful Use Criteria, August 31, 6:45am UTC. healthit.gov/providers-professionals/how-attain-meaningful-use

Accessed August 31, 2012