

**THE ROAD TO
EMR*
noncompliance and
FRAUD
is paved with**

cut
and
paste

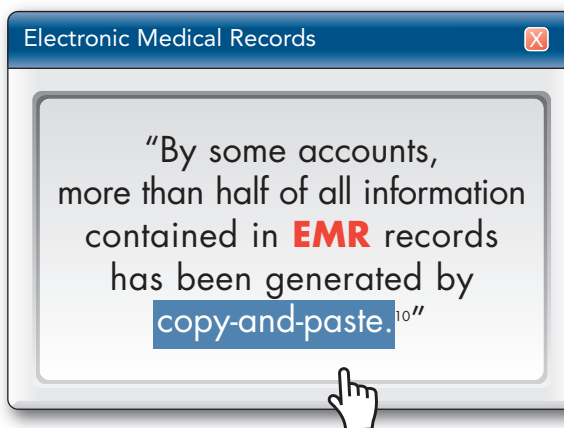


By Leonardo M. Tamburello, Esq.

* Although the terms "EMR" (electronic medical record) and "EHR" (electronic health record) have sometimes been used interchangeably, EMR will be used in this article to focus the discussion on the use of electronic rather than physical media to record patient information. The interchange of information, which is the hallmark of EHR, is a topic for another day.

For more than half a century,¹ electronic medical records (EMRs)² have been heralded as digital replacements for ubiquitous paper charts³ that would allow accurate recording and sharing of patient information with allied healthcare providers and patients themselves.⁴ Despite studies demonstrating that EMR adoption can negatively impact physician performance metrics⁵ (particularly in specialties such as family medicine and pediatrics, which require, more than other specialties, greater data entry, as opposed to retrieval),⁶ incentive programs⁷ have accelerated EMR adoption beyond a critical mass with only limited examination of how electronic records are actually used in the field.

Almost all EMR systems include several forms of input assistance, with the most popular being “copy-and-paste,” use of “macros” (expanded text that is triggered by an abbreviation) and “self-populating” data fields in which, based on the selection of a checkbox, detailed narrative information indicating that the work was done appears in a note without any further action by the author.⁸ In addition, the use of the paste command in a new, blank progress note has become known as a “copy forward.”⁹ Though copy-and-paste and macros originated as word processing functions, they are now shared by many types of devices, operating systems and applications, including most EMRs.



When used appropriately, copy-and-paste can be a valuable, time-saving tool. For example, past medical history, which is verified to be unchanged, may be dealt with in this manner, but should be accompanied by a notation that the information was actually reviewed with the patient, is accurate and is up to date. The far more common practice, however, is to simply duplicate a prior note without editing, attributing or updating.¹⁰ Physician use of copy-and-paste and similar functionality, which generates identical or near-identical chart entries, some with little or no user action, leads to the creation of so-called “cloned documentation.”¹¹ Such practices form the nucleus of emerging areas of risk management in terms of patient safety, professional liability and EMR compliance.

PATIENT SAFETY AND QUALITY OF CARE

By some accounts, more than half of all information contained in EMRs has been generated by copy-and-paste.¹⁰ In one study, publicly available software (originally developed to detect academic plagiarism) was used to analyze 2,068 intensive-care patient notes, related to 135 different patients and written by 62 residents and 11 attending physicians between August 1, 2009, and December 31, 2009. Even though the researchers set the copy detection threshold artificially high to minimize the risk of false positives, they concluded that some 82 percent of residents’ notes and 74 percent of attending physicians’ notes

contained at least 20 percent copied information. These rates are comparable to those found in prior studies that examined non-intensive care unit (ICU) medical documentation and probably *underestimated* the extent of copy-and-paste in the sample examined.⁵

As their usage has spread and their power has grown, EMRs themselves have become insidious vehicles that stealthily perpetuate and compound misinformation.⁴ Through repetition, “everything in the EMR becomes true”¹² to the point where the patient’s chart may lose all narrative cohesion and devolve into a mass of “disorganized, irrelevant or erroneous data.”¹³ These infected records propagate virally without counteragent and lead to results that might seem comical were they not so serious, such as a note persisting for days that a “patient needs drainage, may need OR” after a surgeon had already successfully drained the abscess; this was a case in which an intern copied and pasted a previous note without updating it or citing its source.¹⁴

Despite known causality between copy-and-paste errors in medical records and adverse patient events, the deployment of EMRs continues to proliferate with little scrutiny or oversight.¹⁰ Consequently, a new medical term has been spawned to describe patient harm arising from technology: *e-iatrogenesis*.¹⁵

PROFESSIONAL LIABILITY CONCERNS

HIPAA requires that all EMR systems include the ability to audit and monitor the activities of authorized users.¹⁶ As plaintiffs’ medical malpractice counsel learn of the availability of “information about the information” contained in an EMR, this “metadata” has become an increasingly common target of early discovery.¹⁷ For example, in cases where the timeliness of a treatment or ordering of a diagnostic study is at issue, in addition to hard copies of medical records, a savvy plaintiff’s counsel may request EMR metadata in an attempt to learn intricate details about the client’s treatment that would not be

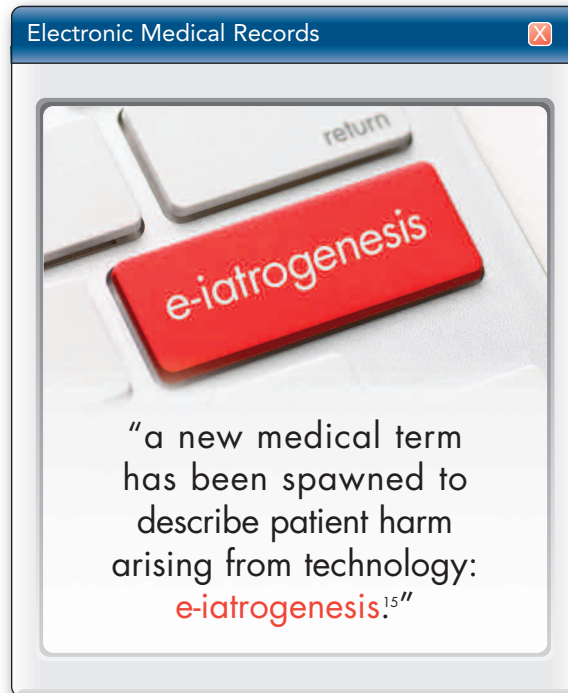
captured by a traditional paper chart and would almost certainly remain beyond the recall of witnesses, including information such as how long it took to chart the patient encounter; the location from which the chart entry was made; whether and when a note included information that had been copied-and-pasted from elsewhere in the EMR; whether a note was edited or added to; precisely what time certain diagnostic results became available, whether they were read and, if so, when and by whom; what other EMR information the user reviewed in the chart encounter; the amount of time spent reviewing each note; and potentially dozens of additional variables that may be captured by the EMR system.

These data represent a potential bounty of discovery for savvy attorneys. Thus, in addition to performing the obvious function as a repository of information, the EMR system is also a powerful monitor of the users who interact with it.

Often, a plaintiff’s counsel requests medical records to evaluate a potential case before filing suit. These requests now

sometimes include EMR metadata within their scope.¹⁸ Armed with such detailed information, the plaintiff’s counsel can evaluate and build a “virtual case” against a practitioner much more efficiently and rapidly than previously possible. Doctors and their defense counsel must be alert to this possibility and sophisticated enough to discern whether this information is included in a document production provided by a plaintiff’s counsel in response to a defense request before the physician’s deposition; the doctor and defense counsel must also be able to intelligently interpret such information for themselves to identify problems or protective information.

Though a doctor is understandably unlikely to remember the specific encounter or course of treatment or his or her own manner of documentation in the months or years between these occurrences and the filing of a professional liability lawsuit concerning them, the persistence of metadata concerning minute details about such



events can create formidable litigation challenges. For example, the unedited self-populated text that follows an “all systems normal” checkbox can lead to uncomfortable questioning if it conflicts with the patient’s primary complaint on the date of that visit. Similarly, if a physician’s note bears striking similarity to others in the EMR, metadata may confirm that it was not independently generated but is instead a product of the “clinical plagiarism” that has been widely acknowledged in the literature for some time.¹⁹

This information in the hands of a skilled plaintiff’s advocate presents unique challenges for a professional liability defense that must be identified and appreciated early in a case. If a doctor gives testimony at the deposition that unwittingly contradicts the omniscient EMR, a liability defense may be compromised.

From a risk management standpoint, the unrestrained use of cut-and-paste, macros and other similar tools in the context of an EMR create significant liability concerns that must be addressed. Risk management officers and insurers should consider developing strategies to minimize this exposure, as outlined below.

EMR-CREATED “CLONED DOCUMENTATION” AND OTHER COMPLIANCE ISSUES

More than one commentator has observed that progress notes exist in their modern form replete with copy-and-paste not to facilitate the transfer of knowledge but to “pass scrutiny” for purposes of reimbursement.^{19, 20} There is a well-documented association between deployment of EMR systems and increased reimbursement. From 2006 to 2010, analysis shows that hospitals that received government incentives to adopt EMR systems experienced a 47 percent overall increase in higher-level evaluation and management (E/M) codes, which is 15 percent greater than hospitals that did not receive similar EMR incentive payments.²¹ Though hospitals claim that EMR systems have allowed them to bill more accurately, federal and state regulators, as well as private insurers such as Aetna and Cigna, have noted the correlation between EMR adoption and increased reimbursements. Consequently, payers now appear poised to closely scrutinize EMR practices, particularly the use of macros and cut-and-paste,²¹ which have resulted in so-called “cloned” submissions.

In 2011, the U.S. Department of Health and Human

Services’ Office of the Inspector General’s (OIG) annual Work Plan announced a new targeted search for identical entries among EMR E/M services based on reports from Medicare contractors concerning “an increased frequency of medical records with identical documentation across services.” Consequently, the OIG stated its intention to “review multiple E&M services for the same providers and beneficiaries to identify... [EMR] documentation practices associated with potentially improper payments.”²²

In 2012, the Secretary of the U.S. Department of Health and Human Services and the Attorney General sent a joint letter to five national healthcare provider associations alerting them to “troubling indications” that providers appear to be using EMRs to “game the system” through the creation of “false documentation.” This letter warned of increased reimbursement scrutiny, including the use of “comparative billing reports” to identify outliers.²³ That same month, it was reported that at least one Medicare contractor had chided doctors that it would deny payment if “cloned documentation” were submitted, while another found that 45 of 100 claims from emergency rooms in Texas and Oklahoma contained “patterns of overcoding” in “template-generated records.”²¹ In addition, the OIG’s 2013 Work Plan again cautions providers: “[We intend to] determine the extent to which CMS made potentially inappropriate payments for E/M services in 2010 and the consistency of E/M medical review determinations. We will also review multiple E/M services for the same providers and beneficiaries to identify electronic health records (EHR) documentation practices associated with potentially improper payments.”²⁴

Separately, the OIG’s investigatory powers have been strengthened by regulatory amendments that expand the Medicare overpayment “look back” period from four to ten years, potentially enabling the federal government to audit and recoup billions in reimbursement already received from Medicare.²⁵

Regardless of the rationale, from the payer perspective, the inappropriate use of EMR tools that result in identical or near-identical documentation suggests the submission of claims for services that were not actually provided at the time of the entry, not provided by the author of the entry or provided by someone (such as a medical student) who may not bill for particular services. As suggested by the OIG and some private insurers, in any of these scenarios, a case can be made that such claims are, at a minimum, improperly

submitted and not reimbursable. In addition to denying payment, the submission of such claims may serve as a basis to initiate a wide-ranging audit, which could lead to punitive sanctions against the institution, practice and/or provider under the federal False Claims Act (FCA) or other state compliance laws.

To be liable under the FCA, a defendant must make a claim or statement that is false or fraudulent that induces the government to pay a claim, with knowledge of the falsity of the statement at the time it was made.²⁶ Although the False Claims Act applies only to federally funded patient encounters, state counterparts available to any insurer whatsoever have become nearly universal. Notably, New Jersey insurers wield a powerful weapon in the form of the Insurance Fraud Prevention Act (IFPA) that may be violated when a provider 1) presents or causes to be presented any written statement in support of a claim for payment, knowing that the statement contains false or misleading information which is material to the claim, or 2) prepares or makes any written statement intended to be presented to an insurance company in support of a claim.²⁷ Treatment notes (or parts thereof) that are duplicated without attribution may run afoul of the IFPA if they give the impression to the payer that the care documented was not given by the charting practitioner at the time. This risk is particularly high when records are serially repeated or “copied forward” across several different patients.

Compensatory damages awardable for any violation of the IFPA include disgorgement of reimbursement related to any tainted claims and the insurance company’s investigation expenses, court costs and counsel fees, which can range into the tens, if not hundreds, of

thousands of dollars.²⁸ If a pattern of five or more related violations is demonstrated, triple damages are mandatory.²⁹ In addition to the insurer’s damages, the State may seek civil penalties up to \$15,000 per violation, plus its own costs and counsel fees. Providers may also be referred to licensing boards for disciplinary action, which can include further monetary penalties, a period of practice supervision, billing monitoring and/or license suspension or outright revocation.^{30,31}

COMPLIANCE STRATEGIES TO SAFEGUARD AGAINST EMR “SLOPPY AND PASTE”

As demonstrated by recent OIG pronouncements, users cannot be left to police themselves in the proper use of EMR systems. Multi-levelled strategies directed at increasing compliant use of EMR input methods are therefore essential.

From a system architecture perspective, users should be forced to encounter “hard stops” at regular intervals when using the EMR that slow down the “click through” process. Compliance officers must gain a firsthand understanding of how their institution’s EMR system is used daily and become active participants in establishing training protocols concerning its proper use.⁸ Education and mandatory requalification on EMR systems should include educating users about risks associated with noncompliant data duplication practices, with an emphasis on revenue protection and quality of patient care. Discussion of the most recent OIG pronouncements should be emphasized, regardless of whether the provider or institution receives direct Medicare or Medicaid reimbursement.



Electronic Medical Records



“medical malpractice attorneys may find a treasure trove of data collected by EMR systems that can be coopted and turned against its very users.”

Risk management should also identify possible non-compliant users through utilization of the EMR's internal self-auditing capabilities to determine which users regularly create duplicate entries in medical records, whether through copy-and-paste, macros or some other functionality. These users can be targeted for additional education and/or closer internal scrutiny before their practices compromise patient care or raise external compliance flags.


Clear policies and procedures concerning the proper use of the EMR's copy-and-paste and similar functionality should be established with the polestar that all EMR entries must accurately represent the author's clinical work performed that day.⁸ If a note relies on, or directly or indirectly references, a prior chart entry (even by the same author), it should do so with clear attribution to the earlier entry by date, time and original author. Clinicians should be encouraged to summarize prior diagnostic testing (i.e., laboratory results, consultation reports, etc.), with proper attribution discussed above rather than wholesale copying of a report into their note.⁸

EMR users must be educated and understand that regardless of the tools used to create their entry, the individual signing the entry is solely responsible for its content. There should be a strict prohibition on 1) copying notes from one patient chart to another ("copying forward"), 2) copying any medical student's notes, which are subject to different reimbursement rules than those of plenary licensed physicians, and 3) any copying associated with the history of the patient's present illness.

As a new and evolving medium, the EMR will not be without growing pains. Early adopting practitioners have shunned the traditional storytelling narrative structure in favor of importing heaps of data into their notes.¹⁰ Traditional payers, including the government, which has long touted the promises of EMRs to increase physician efficiency and reduce costs, have noticed the sharp uptick in reimbursement that accompanies EMR deployment. Despite some shots across the bow, payers have yet to embark on a wide-ranging systemic crack-down on "cloned documentation." Within this context, plaintiffs' medical malpractice attorneys may find a treasure trove of data collected by EMR systems that can be coopted and turned against its very users.

Every practitioner who uses an EMR system, or

institution that deploys one, should take affirmative steps beginning with user education regarding the proper use of shortcuts such as macros and copy-and-paste, or risk learning a harsh lesson through a billing audit or malpractice litigation.

Leonardo M. Tamburello, Esq., is Of Counsel at the law firm of McElroy, Deutsch, Mulvaney & Carpenter, LLP, in Morristown, New Jersey. 

¹ Note: For discussion concerning the longstanding unrealized promises of EMRs and EHRs, see, e.g., National Assembly on School-Based Health Care. (n.d.). *History of the electronic medical record*. www.nasbhc.org/atf/ct/%7BCD9949F2-2761-42FB-BC7A-CEE165C701D9%7D/TA_HIT_history%20of%20EMR.pdf.

² Note: Electronic medical records (EMRs) replicate all aspects of paper documentation such as patient history, physician notes, orders, laboratory results, consultation reports and insurance information. In contrast, an electronic health record (EHR) is an EMR with the capability of sharing data with other providers, practices, systems, platforms and devices. See, Garrett, P., & Seidman, J. (2011, January 4). *EMR vs. EHR: What is the difference?* www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference/.

³ Garrett, P., & Seidman, J. (2011, January 4). *EMR vs. EHR: What is the difference?* www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference/.

⁴ Hartzband, P., & Groopman, J. (2008, April 17). Off the record: Avoiding pitfalls of going electronic. *New England Journal of Medicine*, 358, 1656–1658.

⁵ Thornton, D. (2013, February). Prevalence of copied information by attendings and residents in critical care progress notes. *Critical Care Medicine*, 41(2), 382–388.

⁶ Cerrato, P. (2012, May 7). How to ease EMR frustration. *InformationWeek Healthcare*. www.informationweek.com/healthcare/electronic-medical-records/how-to-ease-EMR-frustration/232901480.

⁷ Note: 42 U.S.C. § 300jj–51 requires the U.S. Department of Health and Human Services to develop recommendations for interoperable and secure standards and protocols that facilitate electronic enrollment of individuals in federal and state health and human services programs. Also, the Medicare and Medicaid EMR Incentive Programs provide incentive payments to eligible professionals, eligible hospitals and critical access hospitals (CAHs) as they adopt, implement, upgrade or demonstrate meaningful use of certified EMR technology. Eligible professionals can receive up to \$44,000 through the Medicare EMR Incentive Program and up to \$63,750 through the Medicaid EMR Incentive Program. See, Centers for Medicare & Medicare Services. (2013, June 26 [updated]).

The official web site for the Medicare and Medicaid Electronic Health Records (EHR) Incentive Programs. www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms.

- ⁸ Association of American Medical Colleges. (2011). *Compliance Officers' Forum: Electronic health records in academic medical center. Compliance advisory 2*. www.aamc.org/download/253812/data/appropriatedocumentationinanehr.pdf.
- ⁹ Note: Though often described as a single function, copy-and-paste is a metaphor for two separate commands, which, when implemented together, permit a user to duplicate text, data, files or objects from one location to another. In the context of EMR usage, users select a section of text, which is then transcribed in a different location when the "paste" command is issued. See, Thornton, D. (2013, February). 383.
- ¹⁰ Hirschtick, R. (2012, July). Sloppy and paste. *Web M&M*. www.webmm.ahrq.gov/case.aspx?caseID=274.
- ¹¹ Bresnick, J. (2013, January 9). EHR patient notes: What's wrong with cloning, anyway? *EHR Intelligence*. <http://ehrintelligence.com/2013/01/09/ehr-patient-notes-what%E2%80%99s-wrong-with-cloning-anyway/>.
- ¹² Hirschtick, R. (2006, May). Copy-and-paste. *Journal of the American Medical Association*, 296(20), 2335–2336.
- ¹³ Siegler, E. (2009, June). Copy and paste: A remediable hazard of electronic health records. *The American Journal of Medicine*, 122(6), 495–496. [Available at www.amjmed.com/article/S0002-9343%2809%2900157-0/fulltext]
- ¹⁴ O'Reilly, K. (2013, February 4). EMRs: "Sloppy and paste" endures despite patient safety risk. *American Medical News*. www.amednews.com/article/20130204/profession/130209993/2/.
- ¹⁵ Thornton, D. (2013, February). 382.
- ¹⁶ 45 C.F.R. § 164.312(b).
- ¹⁷ Note: In *Aguilar v. Immigration Customs Enforcement*, 2008 WL 5062700 (S.D.N.Y. Nov. 21, 2008), the court identified three types of metadata: 1) substantive metadata, meaning application-based information that may contain modifications, edits or comments, that were not necessarily intended for adversaries to see, 2) system-based metadata, which include information automatically captured by the computer system, such as author, date, time of creation and date of modification, and 3) embedded metadata, which consist of text, numbers and content that is directly input but not necessarily visible on output, such as spreadsheet formulas or hyperlinks. *Id.* at *3-*4. Professional liability concerns regarding EMR metadata are usually focused on the second of these categories, system-based metadata, which HIPAA requires to be captured and stored.

- ¹⁸ Note: N.J.A.C. 13:35-6.5(c) requires physicians to provide, upon request, "access to professional treatment records... to a patient" or their authorized representative. Though the minimum contents of such records are enumerated, the term itself is not specifically defined. (See § 6.5(b)(1).) This regulation clearly contemplates the copying of "x-rays or other material within a patient record which cannot be routinely copied or duplicated on a commercial photocopy machine." (See, § 6.5(c)(4)(ii).) This arguably includes metadata such as that required by HIPAA to be captured and maintained.
- ¹⁹ Hartzband, P., & Groopman, J. (2008, April 17). 1656.
- ²⁰ Thornton, D. (2013, February). 387.
- ²¹ Abelson, R. (2012, September 21). Medicare bills rise as records turn electronic. *The New York Times*. www.nytimes.com/2012/09/22/business/medicare-billing-rises-at-hospitals-with-electronic-records.html?pagewanted=all.
- ²² U.S. Department of Health and Human Services, Office of Inspector General. (2011). *Work Plan Part I, Medicare Part A and Part B*. 1-14. http://oig.hhs.gov/publications/workplan/2011/WP01-Medicare_A+B.pdf.
- ²³ Sebelius, K., & Holder, E. (2012, September 24). [Letter from Secretary of the U.S. Department of Health and Human Services and the Attorney General U.S. Department of Justice to the Chief Executive Officers of the American Hospital Association, Federation of American Hospitals, Association of Academic Health Centers, Association of American Medical Colleges and National Association of Public Hospitals and Health Systems]. [Available at <https://s3.amazonaws.com/s3.documentcloud.org/documents/439406/hhs-doj-health-associations.pdf>]
- ²⁴ U.S. Department of Health and Human Services, Office of Inspector General. (2013). *Work Plan Part I: Medicare Part A and Part B*. 25. http://oig.hhs.gov/reports-and-publications/archives/workplan/2013/WP01-Mcare_A+B.pdf.
- ²⁵ 42 C.F.R. § 401.305(g).
- ²⁶ *United States v. The Boeing Company*, 100 F.Supp. 2d 619, 625-626 (S.D. Oh. 2000).
- ²⁷ N.J.S.A. 17:33A-4.
- ²⁸ N.J.S.A. 17:33A-7(a).
- ²⁹ N.J.S.A. 17:33A-7(b).
- ³⁰ N.J.S.A. 17:33A-5.
- ³¹ N.J.S.A. 45:1-14.