Copy & Paste—CMS To The Rescue!

BY CINDY PARMAN, CPC, CPC-H, RCC

Electronic health records (EHRs) can help providers correctly document and code the services they provide. Yet physicians struggle to use EHRs to help ease documentation burdens. Further, providers must ensure that their EHR notes do not take on a problematic uniformity.[1] In the same way that medical coders want their codes to tell the patient's story, physician documentation should provide an accurate picture of the patient's medical condition(s), treatment provided, and response to care.

According to Medicare, the problem arises around documentation that is worded exactly like or similar to previous entries in the same patient chart or across medical records for patients with the same medical conditions.[2] This may include pre-printed templates, fill-in-the blank forms, check-off boxes, copy and paste, or information defaulted (brought forward) from other medical record documents. An article in *FierceEMR* states:[3]

> *Most physicians are taking advantage of their copy and paste function in their electronic health records and copying progress notes rather than creating new, original ones, according to a new study published in the journal* Critical Care Medicine.
>
> *The study examined 2,068 progress notes by 62 residents and 11 attending physicians of 135 intensive care unit patients in a medical center in Cleveland, using plagiarism detection software. The researchers found that more than four-fifths (82 percent) of the residents and three-fourths (74 percent) of the attendings' notes contained at least 20 percent of copied information. While the residents authored more copied notes, they copied a bit less information than the attendings (55 percent to 61 percent).*
>
> *After a day or more off, a whopping 94 percent of the attendings copied from their own prior notes, and two-thirds (66 percent) of the residents did so.*

Documentation short-cuts can create difficulty in supporting medical necessity, determining the complexity of care provided, or differentiating treatment from one patient to another. Unlike a note written on paper, a note written in the EHR can be generated by using information that was recorded elsewhere and is imported from either within or outside the EHR, such as when sections of a document are copied from one file and pasted into another.

Fraud Concerns

According to *The Intersection of EHRs and Fraud and Abuse*, national dialogue surrounding EHRs has turned toward the potential for fraud and abuse:[4]

> *If not used correctly, computers have given us the power to make mistakes in large quantities at the speed of light. So, depending on the design of an EHR and how it is used by the provider, the electronic environment can certainly make it much easier to generate the amount of documentation required to support a higher-level code or to make medical necessity appear to be met when, in fact, neither case can be supported.*
>
> *Since the idea is to lessen the crushing workload that many doctors are under by letting the system "do the work," the potential exists to lose a crucial level of controls, i.e. the vast majority of providers who would never abuse the system on purpose.*

In September 2012 the Department of Health and Human Services (DHHS) and the Department of Justice (DOJ) issued a joint letter stating that there were indications some healthcare providers were using EHRs to clone medical record documentation on Medicare claims to boost payments. The letter, signed by Secretary Kathleen Sebelius and Attorney General Eric Holder, states in part:[5]

> *A patient's care information must be verified individually to ensure accuracy. It cannot be cut and pasted from a different record of the patient, which risks medical errors as well as overpayments.*

This letter followed a *New York Times* article that detailed how the use of EHRs may be a contributing factor in higher Medicare billings. Rich Umbdenstock, chief executive of the American Hospital Association (AHA), responded on behalf of the AHA, "We agree that the alleged practices described in your letter, such as so-called 'cloning' of medical records and 'upcoding' of the intensity of care, should not be tolerated."[6]

2012 CMS Instructions

On Dec. 10, 2012, CMS issued revised instructions stating that while template use is not prohibited, the agency does not approve or endorse any templates. In addition, CMS discourages the use of templates that provide limited options for the collection of information, such as check boxes or predefined answers, or limited space to enter information. According to CMS:[7]

Some templates provide limited options and/or space for the collection of information such as by using "check boxes," predefined answers, limited space to enter information, etc. CMS discourages the use of such templates. Claim review experience shows that that limited space templates often fail to capture sufficient detailed clinical information to demonstrate that all coverage and coding requirements are met.

Physicians should be aware that templates designed to gather selected information focused primarily for reimbursement purposes are often insufficient to demonstrate that all coverage and coding requirements are met. This is often because these documents generally do not provide sufficient information to adequately show that the medical necessity criteria for the item/service are met.

If a physician chooses to use a template during the patient visit, CMS encourages them to select one that allows for a full and complete collection of information to demonstrate that the applicable coverage and coding criteria are met.

Add to the audit factor the concern that as EHRs become more interconnected, errors resulting from their use can be amplified and affect a larger group of individuals.[8] Once EHR information is transmitted using health information exchanges, any incorrect, incomplete, or templated information entered into the record will be widely distributed. As a result, the scale of the problem has changed; what used to be a single data entry or incorrect statement can now cascade into multiple records.

In addition, risks of cloned or copied medical record information include the possibility that a note will be populated with outdated, conflicting, incomplete, or inaccurate information. Cloned notes may also be repetitive, inconsistent, or identical; these notes do not assist in the care of the patient and over time may be ignored by other staff due to the presence of outdated or stagnant information.

Last, notes that continue to build over time with the constant addition of information become cluttered; in this situation, new or pertinent information may be overlooked or may not be easily accessible by other service providers.

2013 OIG Report

The next chapter in the documentation saga was triggered by a December 2013 Office of Inspector General (OIG) report, "Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology."[9] While the OIG report focuses on hospital EHRs, physicians and freestanding centers will likely be bound by the documentation policies that result from this study. The OIG states, in part:[9]

EHRs replace traditional paper medical records with computerized recordkeeping to document and store patient health information. Experts in health information technology caution that EHR technology can make it easier to commit fraud.

This study determined how hospitals that received EHR Medicare incentive payments, administered by the Centers for Medicare & Medicaid Services, had implemented recommended fraud safeguards for EHR technology.

For this study, the OIG administered an online questionnaire to the 864 hospitals that received Medicare incentive payments as of March 2012 and received a 95 percent response rate. The questions focused on the presence of safeguards related to audit functions, user authorization, access, and data transfer. In addition, the OIG conducted onsite structured interviews and observed an EHR demonstration in eight hospitals. Last, the agency conducted surveys with four EHR vendors and asked them "the extent to which they had incorporated the recommended fraud safeguards into their products."

As a result of this study, the OIG determined that nearly all hospitals with EHR technology had the recommended audit functions in place, but that hospitals might not be using these functions to their full extent. In addition, only about one fourth of hospitals had policies regarding the use of copy-paste features; which, if used improperly, could pose a vulnerability for fraud. According to the OIG:[9]

Copy-pasting, also known as cloning, allows users to select information from one source and replicate it in another location. When doctors, nurses, or other clinicians copy-paste information but fail to update it or ensure accuracy, inaccurate information may enter the patient's medical record and inappropriate charges may be billed to patients and third-party healthcare payers. Furthermore, inappropriate copy-pasting could facilitate attempts to inflate claims and duplicate or create fraudulent claims.

Although the copy-paste feature in EHRs can enhance efficiency of data entry, it may also facilitate attempts to inflate, duplicate or create fraudulent healthcare claims.

In 2006 the Office of the National Coordinator (ONC) for Health Information Technology contracted with RTI International to develop recommendations to enhance data protection, including increasing data validity, accuracy, and integrity as well as strengthening fraud protection in EHR technology. The resulting recommendations addressed several types of vulnerabilities, including copy-paste and overdocumentation. RTI recommendations require:

1. The use of an audit log function and specify audit log operation and content for tracking EHR updates.
2. The methods (i.e., copy-paste, direct entry, import) for any EHR update be documented and tracked.
3. The user ID of the original author be tracked when an EHR update is entered "on behalf" of another author (i.e., distinguish between entries made by an assistant and a provider).
4. That original EHR documents be retained after they are signed off and modifications be tracked as amendments.
5. That EHR technology not prompt an EHR user to add documentation, but be able to alert a user to inconsistencies between documentation and coding.

All four EHR vendors surveyed by the OIG indicated that they provided standard product implementation training, but that hospitals do not commonly request additional audit log training. Of note, 49 percent of the hospitals responding to the OIG survey indicated that they track the date, time, and user ID of the original author when data are copied. In addition, 44 percent of hospitals already track the method used when data are entered into the EHR (such as direct text entry, speech recognition, automated, or copy-paste). However, none of the hospitals surveyed analyzed their audit logs to prevent or detect fraud, for example, by identifying duplicate or fraudulent claims and inflated billing. Last, only 24 percent of hospitals had policies in place regarding the use of copy-paste in the EHR.

The OIG stated that CMS must do more to ensure that all hospital EHRs contain safeguards and that hospitals use them to protect against electronically enabled healthcare fraud. Recommendations from the OIG included development of a comprehensive plan to address fraud vulnerabilities in EHRs. In addition, the OIG made a specific recommendation that CMS develop guidance on the use of the copy-paste feature in EHR technology, and CMS stated that it will develop guidelines to ensure that this feature is appropriately used. The CMS response states, in part:[9]

- CMS is planning to work with ONC to develop a comprehensive plan to detect and reduce fraud in EHRs.
- CMS is conducting audits as a method to reduce fraud, waste, and abuse in the EHR Incentive Programs. Some of these pre-payment audits will be random and some will target suspicious or anomalous data.
- CMS will develop appropriate copy-paste guidelines to ensure that this feature is used appropriately for enhancing clinical efficiency.

Last, the OIG stated that it will release a companion report to the December 2013 document that describes the program integrity practices CMS implements in response to these recommendations.

What Should Providers Do?

First, identify the documentation shortcuts, including copy and paste, used in the EHR at all practice or hospital locations. Additional recommendations for facilities and physicians to consider include:

1. Ask the hard questions when a vendor states that the EHR will increase reimbursement, such as how will that happen? Will it be through increasing accuracy and detail or some other mechanism?
2. Implement strong compliance controls to constantly monitor the bills submitted, track coding trends, etc. For example, it may be prudent to audit documentation for inconsistencies or similarities to prior notes.
3. Include compliance training for all staff members in every meeting, whether the practice or facility is in the process of implementing the EHR or for purposes of ongoing review.
4. Establish written policies for automatic field population, copy and paste, the use of templates, and other documentation shortcuts.
5. Ensure that there is a method for EHR users to communicate documentation concerns and errors in the medical records.

The following publicly available resources from the American Health Information Management Association (AHIMA) will help with establishing specific internal guidelines:

- *The Legal Health Record: Copy and Paste Guidelines.* (http://campus.ahima.org/audio/2009/RB111709.pdf)
- *Auditing Copy and Paste.* (http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_042416.hcsp?dDocName=bok1_042416).

Continually monitor medical record documentation—whether performed via dictation, dynamic documents, or other electronic method—to ensure that any templates in use are correct, complete, and compliant. Further, educate physicians and other staff on the proper use of templates, the difference between a template and a cloned note, and the need for complete and accurate medical record documentation. OI

Cindy Parman, CPC, CPC-H, RCC, is a principal at Coding Strategies, Inc., in Powder Springs, Ga.

References

1. Lojewski T. Copy that? Not so fast. CodeWrite. Nov. 2012. Available online at: http://newsletters.ahima.org/newsletters/Code_Write/2012/November/November12_CW.html. Last accessed April 9, 2014.
2. CMS. Chapter 4: Benefit Integrity. Medicare Program Integrity Manual. Available online at: http://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/pim83c04.pdf. Last accessed April 9, 2014.
3. Hirsch MD. Copying and pasting of EHR info "common." *FierceEMR*. Jan. 7, 2013. Available online at: http://www.fierceemr.com/story/copying-and-pasting-ehr-info-common/2013-01-07. Last accessed April 9, 2014.
4. HIMSS. *The Intersection of EHRs and Fraud and Abuse*. Nov. 19, 2012. Available online at: http://www.himss.org/News/NewsDetail.aspx?ItemNumber=2871. Last accessed April 9, 2014.
5. DHHS and DOJ. Letter to the Obama Administration. Available online at: http://www.nytimes.com/interactive/2012/09/25/business/25medicare-doc.html?_r=2&. Last accessed April 9, 2014.
6. AHA. Letter to DHHS Secretary and the U.S. Attorney General. Available online at: http://www.aha.org/advocacy-issues/letter/2012/120924-let-hhsdojehrbilling.pdf. Last accessed April 9, 2014.
7. CMS. CMS Manual System. Pub 100-08 Medicare Program Integrity. Transmittal 438. Available online at: http://www.cms.gov/Regulations-and-Guidance/Guidance/Transmittals/Downloads/R438PI.pdf. Last accessed April 9, 2014.
8. Baum S. EHRs may turn small errors into big ones. MedPage Today. Dec. 6, 2012. Available online at: http://www.medpagetoday.com/PracticeManagement/InformationTechnology/36474. Last accessed April 9, 2014.
9. OIG. Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology: Complete Report. Available online at: http://oig.hhs.gov/oei/reports/oei-01-11-00570.asp. Last accessed April 9, 2014.