

MEDICARE COMPLIANCE

Anti-Fraud Features Coming to EHR Systems; Tools Aim to Prevent Claims Manipulation

Electronic health record (EHR) systems may soon contain features that will assist in the prevention and detection of billing errors and fraud. Fifteen proposed anti-fraud requirements have been drafted under the auspices of the U.S. Office of the National Coordinator (ONC) for Health Information Technology, and could be headed for inclusion in EHR systems.

ONC awarded RTI International of Research Triangle Park, N.C., a half-million-dollar contract to develop "model anti-fraud requirements for EHRs" between November 2006 and March 2007. RTI was charged with creating a working group comprised of people with the expertise necessary to create the anti-fraud requirements, says Matt McMullen, a CMS subject matter expert and health insurance specialist.

"The group tried to lay the groundwork for fraud and abuse detection and prevention measures in EHRs," McMullen tells *RMC*. "Building fraud detection into EHRs at these early stages will allow law enforcement, providers and patient advocacy groups to have some degree of confidence that it will operate effectively. It may be much more expensive and difficult to try to add some of these fraud prevention and detection features later when various other standards are already in place and may not be congruent with these recommendations."

These anti-fraud requirements would not be government mandated. Instead, they will become part of EHR vendor certification criteria, explain McMullen and Colleen McCue, the RTI project director and a senior research scientist. However, since vendors usually seek a Good Housekeeping seal of approval from their certification bodies, the anti-fraud requirements, if finalized, would become standard operating procedure. "When you see a process is certified, you know it represents the best standards," McCue notes. It becomes a sort of *de facto* requirement, the way compliance programs are.

How did all this come about? ONC is tackling all kinds of health information technology (HIT) standards, including privacy and security, as part of its mandate to achieve universal EHR usage by 2014. Fraud and abuse more recently captured HIT experts' attention when it became apparent there was "a rare opportunity" to insert prevention and detection functions into the DNA of EHR systems instead of adding them later, McMullen says.

So ONC embarked down this path by forming the model requirements executive team (M-RET) executive

committee and then hiring RTI International last year. They came up with a draft and put it out for public comment. McMullen says RTI received a lot of comments from stakeholders, including law enforcement agencies, vendors, the American Medical Assn., American Hospital Assn., citizen groups and others.

"Overall, the comments from [stakeholders] were supportive," McMullen says. "There were more pluses than negatives."

Requirements Get Very Detailed

The requirements cover a range of risk areas (see box, p. 7). There is a requirement for evaluation and management coding, which says the system may inform physicians when their E&M codes don't match their documentation, but they can't tell physicians to add documentation. "It is appropriate for EHRs to calculate an evaluation and management (E&M) code from the encounter data which has been entered and to indicate the basis for that calculation. However, it is not appropriate to suggest to the provider that certain additional data, if entered, would increase the level of the E&M code," the draft states.

In addition, there is a requirement on copying notes (also known as cloning or cutting and pasting). When physicians copy an existing note about a patient and paste it into another chart entry as a shortcut with updating required (*RMC 12/2/06, p. 1*), they must retain the date, time and user stamp of the original author, the requirement states. If it's copied from another patient, the original patient ID should not be kept. *The draft rationale:* "Copying and pasting all or a portion of a previous note is a provider efficiency tool. This process can be abused by appearing to attribute observations made by a previous provider to the current provider. If the intent is simply to provide common terminology or phraseology for reuse, templates or defaults may be used for this purpose."

The draft also contains a long, detailed requirement for audit functions and features.

Another requirement: provider identification mechanisms that make sure the national provider identifier (NPI) is used to prevent common fraud schemes involving the theft of provider numbers to submit false claims, according to the draft. There's a requirement involving user access authorization, which explains that "the health care entity bears responsibility for assuring that all indi-

viduals authorized to access the EHR have the requisite credentials for the services they provide.”

M-RET and RTI International have walked a fine line in trying to achieve the goal of building in tools that prevent medical-record and claims manipulation for the purpose of committing fraud while not alienating vendors with excessive costs, McMullen says.

Next up, RTI International will work with the certification bodies on integrating the anti-fraud requirements into their certification criteria, says McCue. The bodies are the Certification Commission for Health Information Technology (CCHIT) and the complementary Health Information Technology Standards Panel (HITSP).

More to It Than Anti-Fraud

“It’s our hope that vendors and providers will start looking at the recommendations and hopefully will adopt them early,” she says.

McCue says that although the requirements are termed “anti-fraud,” there is much more to it. “What has been recommended is about maintaining good data — reliability, accuracy, recommendations to protect the integrity of the data,” she says.

For example, one of the requirements is the “integrity of electronic health record transmission.” It requires the EHR system to be able to “transmit clinical information to

other information systems using standards that retain the available level of coding and structure, such as the HL7 Clinical Data Architecture.” The rationale, according to the draft document: “Intentional or unintentional modification of records can occur during the transfer from one system to another. Systems must be able to irrefutably ensure that transmission of EHR information has occurred in an unaltered state.”

McCue also emphasizes that the requirements address the link between fraud and quality. Patient safety can be jeopardized by medical identity theft. When medical records are altered to reflect the poser’s diagnoses, procedures and medications, that can have a ripple effect with potentially disastrous consequences (e.g., the patient who steals a real patient’s identity says he had his appendix out so when the real patient shows up with all the signs of rupturing appendix, physicians assume it’s something else because the medical records say he already had it removed).

That’s why the draft includes a patient identification category, which requires the “capability to capture a unique physical patient identifier, such as a photo and/or a biometric in the EHR and capture means used by a practice to validate identification by 2009.”

Contact McCue at cmccue@rti.org and McMullen at matthew.mcmullen@cms.hhs.gov. E-mail comments on the anti-fraud requirements to RTI at antifraud@rti.org. ✧

Anti-Fraud Features for Electronic Medical Records

Here are more fraud prevention and detection features designed for electronic medical record (EMR) systems. They were developed by the U.S. Office of National Coordinator for Health Information Technology, and are part of draft requirements for EMR systems, approved Jan. 29 (see story, p. 1).

◆ **Documentation process issues:** The requirement calls for the “ability to view an audit version of each encounter note, which indicates the method of entry for each data element. Specifically differentiate the following: (1) Direct entry via integrated hardware keyboard or mouse; (2) Voice recognition; (3) Automated, machine-entered default information; (4) Pre-created documentation via form or template; (5) Copy/paste; (6) Copy forward previous note contents; and (7) Dictation/Transcription.

The rationale for a requirement in this arena, the draft says, is that “EHRs provide various tools that enable a provider to be more efficient of his/her time when documenting an encounter. These include the use of defaults, templates, copying and other tools. These are legitimate benefits of using an automated system; however they could be subject to fraud or abuse. Having an audit version of the EHR which

indicates which of these tools were used could enable detection of patterns of abuse or fraud.”

◆ **Record modification and signature:** “Requires retention of original documents and any amendments after “signature event” (including automatic “closing” of record).” The rationale says, among other things, that “retaining an audit trail of changes after this event prevents fraudulent alteration of the record at a later time.”

◆ **Patient involvement in anti-fraud:** Require patients’ access to their own EMRs and disclosure logs and let them comment in EMRs. The rationale: “Patients can be a potent force in combating fraud. However, they must be given the tools to do so.” That’s one purpose of giving patients an explanation of benefits form, the draft says. But it adds, “Direct review of an encounter note which was used to generate a claim would be an even stronger tool for prevention and detection of fraud.”