Reinhart

OIG Companion Reports Indicate Increased Attention to EHR Fraud Prevention and Detection

The U.S. Department of Health and Human Services (HHS) Office of Inspector General (OIG) recently released two companion reports examining the use of certain recommended fraud controls in electronic health records (EHR). The reports concluded neither providers nor the Centers for Medicare & Medicaid Services (CMS) or its contractors were comprehensively addressing the new fraud vulnerabilities created by the transition from paper records to EHRs. The reports recommend increased efforts and procedures for providers and CMS to prevent and detect fraud. The increased OIG focus on fraud vulnerabilities associated with EHRs reinforces the need for providers to adopt and implement effective EHR policies and procedures, specifically policies and procedures addressing EHR audit logs and copy-paste practices.

POSTED:

Feb 8, 2014

RELATED PRACTICES:

Health Care

https://www.reinhartlaw.com/practices/health-care

The December 2013 Report

The first OIG report was released in December 2013 and focuses on assessing the extent to which providers that receive EHR Medicare incentive payments implemented recommended fraud safeguards. Namely, it looks at the use of audit functions, user authorization and access controls, the adoption of recommended data transfer standards, the use of patient involvement in anti-fraud activity and the implementation of policies to address inappropriate copy-paste functions in EHRs. The report's overall findings were mixed, highlighting both successes and shortcomings of providers' adoption of fraud safeguards.

- **Audit Functions**. The report describes the crucial role audit logs play in preventing fraud by monitoring EHR user activity. While the report finds nearly all hospitals had in place recommended audit functions and even analyzed the logs to ensure EHR privacy, many were not using the functions to their full extent, with few analyzing them to detect and prevent fraud and abuse. The report expresses further concern over the apparent ability of many users to edit and delete audit logs, which compromised the log's effectiveness.
- **EHR Accuracy Mechanisms**. Additionally, the report finds that all hospitals employed a variety of recommended user authorization and access controls, and nearly all used recommended data transfer safeguards. Nevertheless, only one-half of hospitals had implemented recommended tools to include

patient involvement in anti-fraud efforts, and only one-quarter of hospitals had policies regarding the use of copy-paste functions in EHRs.

- **Copy-Paste Policies**. Even though one-quarter of hospitals have a copy-paste policy, the report expresses concern that even such hospitals seem to have very little control over its use. Copy-paste, also known as cloning, allows users to select information from one source and replicate it in another location. The function is often used to increase data entry efficiency. However, OIG's concern over the practice is sourced in the potential for inflated claims and duplicate or fraudulent claims when information is cloned but not updated or reviewed to ensure accurate information and charges. The policies reviewed in the report varied from having the EHR user verify the accuracy of the data or citing the source of the data to advising against "indiscriminately copy-pasting." Interestingly, the report cites feedback from both providers and vendors on their inability to customize the function.

In light of the report's findings, OIG made several recommendations, including changing the certification or Meaningful Use criteria to require that audit logs be operational whenever EHR technology is available for updates or viewing—meaning disabling edit and delete functions. The report also recommends CMS strengthen collaborative efforts to develop a comprehensive plan to address the fraud vulnerabilities in EHRs. Most importantly, the report recommends that CMS develop guidance on the use of the copy-paste feature in EHR technology. While CMS agreed to develop and issue such guidance, it did not provide an anticipated date on which providers can expect to see the guidance.

The January 2014 Report

The second report was released in January 2014 and assesses the extent to which CMS and its contractors implemented program integrity practices in light of EHR adoption. Highlighting the new fraud vulnerabilities created by the transition from paper records to EHRs, the report addresses the need for CMS and its contractors to adjust their techniques for identifying improper payments and investigating fraud. The report identifies that CMS and its contractors have adopted very few practices in response to the transition. Few contractors review EHRs any differently than paper records and some contractors do not even have the ability to determine whether a provider has copied language or overdocumented within a medical record.

OIG recommends that CMS provide guidance to its contractors on detecting fraud associated with EHRs and further calls on CMS to direct its contractors to use

provider audit logs for fraud detection. CMS concurred in part to increasing the use of provider audit logs, stating that using audit logs is part of its comprehensive approach, but clarifying that audit logs may not be appropriate in every circumstance, and requires additional training.

Best Practices

In response to these reports, hospitals and health systems should adopt EHR policies and procedures to address the underscored vulnerabilities. Specifically, hospitals and health systems should consider:

- Implementing policies on audit logs, including edit and delete functions;
- Implementing policies discouraging indiscriminate copy-pasting by encouraging EHR users to verify information and charge accuracy, and to document the source of the data;
- Discussing fraud and abuse auditing capabilities with their EHR vendor;
- Adding spot audits of EHRs to their annual audit plans; and
- Providing additional EHR training to physicians and coders.

Reinhart's Health Care team is available to assist your hospital or health system in the development and adoption of electronic health record policies and procedures, or to consult with you regarding any other legal or regulatory issues. Please feel free to contact Larri Broomfield, Heather Fields, or any member of Reinhart's Health Care team or your Reinhart attorney to discuss any questions or concerns related to your hospital or health system.