

FEDERAL CIVIL ENFORCEMENT

Expert Analysis

## Fraud and Abuse Enforcement Goes High Tech

On May 31, 2017, the U.S. Department of Justice announced a \$155 million settlement with electronic health records (EHR) company eClinicalWorks (eCW). The settlement resolved allegations that eCW violated the False Claims Act (FCA) by falsely certifying that its software included certain design features and functionality. The settlement marks the first resolution of an FCA case related to an incentive program that has made over \$30 billion in Medicare and Medicaid incentive payments available to health care providers to promote the use of EHRs and raises questions about the potential exposure of EHR companies to FCA liability as a result of issues with software design and functionality.

Shortly after the eCW settlement was announced, the Department of Health and Human Services (HHS), Office of Inspector General (OIG) issued an audit report (the OIG report) estimating that the Center for Medicare and Medicaid Services (CMS) paid \$729.4 million in EHR incentive payments to health care providers who did not meet the



By  
**Richard  
Strassberg**



And  
**William  
Harrington**

criteria for demonstrating meaningful use of their EHR technology and were thus not entitled to such payments. The primary issue cited in the OIG report is the inability of the health care providers to provide documentation supporting their attestations that they met the requirements to establish meaningful use of their EHR software.

The eCW settlement and the OIG report will likely prompt a significant increase in enforcement activity related to EHR incentive payments. We review these developments, their ramifications, and steps EHR companies and health care providers can take to protect themselves from liability related to EHR incentive payments below.

### Medicare, Medicaid Incentives

In 2009, to promote the adoption of EHRs, as part of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), Congress created an incentive program

under Medicare and Medicaid to reward health care providers for adopting and demonstrating meaningful use of certified EHRs. Under the incentive program, physicians and other eligible professionals such as dentists and podiatrists are eligible for a total of up to \$43,720 over five years from Medicare or \$63,750 over six years from Medicaid.

To qualify for incentive payments, eligible professionals must

---

The eCW settlement and the OIG report will likely prompt a significant increase in enforcement activity related to electronic health records incentive payments.

demonstrate “meaningful use” of “certified” EHR technology. Eligible professionals demonstrate meaningful use by providing an attestation to CMS that they have met a number of objectives and measures related to their use of a certified EHR such as performing computerized order entry for a certain percentage of patients.

The National Coordinator for Health Information Technology (ONC) designates authorized certification bodies (ACBs) to certify EHR technology. To obtain certification, an EHR vendor must certify to an ACB that its

---

RICHARD STRASSBERG and WILLIAM HARRINGTON are partners at Goodwin Procter. Goodwin partner ROGER COHEN, whose practice focuses on health care law, including the defense of health care providers and health IT companies in False Claims Act investigations, co-authored this column.

product satisfies certification criteria and subject the product to testing by an ACB.

### Allegations of eCW Complaint

The most eye-catching allegations of the complaint against eCW relate to eCW's purportedly false certification to its ACB in April 2013 that its EHR used a standardized drug vocabulary called RxNorm for transmitting electronic prescriptions that specified each unique drug, formulation, and dosage. eCW allegedly led the ACB to believe that it had implemented RxNorm by reviewing the publicly available test scripts used by the ACB, identifying the 16 drugs for which it would need to generate a prescription during testing, and "hardcoding" the 16 RxNorm codes into its software so that the software would use the RxNorm codes when transmitting electronic prescriptions during the test. According to the complaint, instead of using RxNorm, eCW's software actually relied on proprietary drug identifiers and National Drug Codes (NDCs). Allegedly, in some cases, eCW's software did not send accurate NDC codes when transmitting medication orders, and eCW was alerted to this problem by a "third party business partner" in 2014 and 2015.

The complaint also alleges a number of other deficiencies in the eCW software. These include the use of laboratory names instead of Logical Observation Identifiers Names and Codes to facilitate the transmission of patient education information; a failure to transmit Systematized Nomenclature of Medicine-Clinical Terminology codes, standardized codes used to identify medical conditions; a failure to allow the batch export of patient summaries; failure of its software to meet audit log requirements under certain conditions; a failure to record diagnostic imaging orders in certain situations; and failure to perform certain checks for drug

interactions and allergies. There is no allegation that eCW engaged in any "hardcoding" to pass tests related to these criteria or that the ACB tested for these criteria.

The complaint alleges that as a result of eCW's representations that its product was certified, health care providers using eCW "unknowingly" submitted tens of thousands of claims falsely attesting that they had used certified EHR technology and were thus eligible for incentive payments.

In addition to the software issues, the complaint also alleges that eCW violated the Anti-Kickback Statute (AKS) by paying kickbacks to customers to recommend its product

---

Eligible professionals who have reason to believe that they previously received EHR incentive payments without meeting meaningful use objectives should also consider whether they are obligated to report and return such payments pursuant to the Medicare Part A and B overpayment rule.

to other customers via \$500 referral fees; paying existing customers to host prospective customers with the payments being based on the number of users at the prospective customer's facility; payments of up to \$250 to customers to provide references; and providing consulting payments, speaker fees, gift cards, iPads, meals, travel, and entertainment to "influential" customers who promoted the software.

### The OIG Report

The OIG report summarizes the results of an audit of payments made under the EHR incentive program from May 2011 through June 2014. The audit consisted of a review of a sample of a total of approximately

\$2.5 million in payments made to 100 health care providers (out of a total of approximately \$6.1 billion in payments made to 250,000 health care providers in the audit period). OIG determined that 14 of the health care providers were unable to provide documentation supporting their meaningful use attestation. These providers received a total of \$291,000 in EHR incentive payments.

With respect to the 14 health care providers, OIG determined:

- six could not provide a security risk assessment, which is a "core measure" that must be met to be eligible for an EHR incentive payment;
- four could not provide support for meeting the "menu" measure of generating at least one report listing patients with a specific condition;
- three could not provide documentation of patient encounter data to support their attestation;
- one provider based his attestation on 90 days of encounter data instead of a full calendar year as required; and
- one provider did not have at least 50 percent of his patient encounters at a location equipped with certified EHR technology.

OIG's recommendations include that CMS review incentive payments to identify health care providers who did not meet meaningful use measures to attempt to recover the \$729 million in estimated inappropriate payments and conduct a further review of a random sample of claims that may have been made after the June 2014 end of the audit period.

In comments responding to the OIG report, CMS stated that it would implement "targeted risk-based" audits to strengthen the integrity of the EHR Incentive Program, but did not accept the recommendation to attempt recovery of the \$729 million in estimated inappropriate payments. CMS did not explain the basis for its position in its letter commenting on OIG's findings.

## Discussion

The significant eCW settlement and the OIG report will almost certainly prompt an increase in enforcement activity related to the EHR incentive program. One issue that will likely be a subject of focus in enforcement actions against EHR companies is the extent to which defects in software design and functionality can serve as a basis for liability under the FCA. While the complaint against eCW included relatively salacious allegations that eCW “hardcoded” its software so that when the software was tested it would appear to have certain functionality related to e-prescribing that it did not have, the complaint also included more mundane allegations that the software did not meet various technical requirements. Future cases will likely result in litigation of whether software issues like the more mundane issues discussed in the eCW complaint are sufficiently material to create FCA liability.

Future litigation is also likely to focus on whether allegedly false certifications of compliance were made “knowingly.” A person acts “knowingly” under the FCA if he or she has actual knowledge of information or acts with deliberate ignorance or reckless disregard of the truth or falsity of information. The eCW complaint cited a litany of customer complaints and internal email about the various technical software issues to support the claims that by attesting that its software met applicable certification criteria, eCW knowingly caused the presentation of false claims for incentive payments by eligible professionals. In light of the eCW settlement, EHR companies should carefully review complaints related to the design and operation of their software and any related legal obligations.

ONC promulgated new regulations in October 2016 that, among other things, require ACBs to post the results of their product testing and

surveillance on ONC’s website. EHR companies should review their surveillance results and consider their obligations to address any issues identified through such surveillance.

The corporate integrity agreement entered into by eCW in connection with its settlement underscores the government’s focus on software defects as a compliance issue. Specifically, in addition to more typical responsibilities, the Compliance Officer’s responsibilities under eCW’s corporate integrity agreement include “timely and effective identification, notification, reporting, and remediation of any software defects, usability problems, deficiencies, or other issues that may present a risk to patient safety or that may be inconsistent with any applicable requirement of the ONC Health IT Certification Program[.]” The corporate integrity agreement similarly requires eCW to appoint a Compliance and Quality Assurance Committee including, among others, representatives from among senior personnel responsible for patient safety activities and design, development, testing and certification of the EHR software, and customer/user support. EHR companies and other health IT companies should consider appointing Compliance Officers and creating Compliance and Quality Assurance Committees and assigning them responsibilities like those assigned under eCW’s corporate integrity agreement.

EHR and other health IT companies should also carefully review their marketing activities to ensure compliance with the AKS.

Recipients of EHR incentive payments should consider taking steps to protect against alleged FCA violations and the recovery of their EHR incentive payments. Among other things, recipients of EHR incentive payments should be sure to maintain documentation substantiating their attestations of meaningful use.

While CMS did not accept OIG’s recommendation to attempt recovery of the \$729 million in estimated inappropriate payments, it did commit to implement “targeted risk-based” audits to strengthen the integrity of the EHR Incentive Program. Auditors will almost certainly review documentation of the basis for attestations of meaningful in these audits and seek to recover payments when eligible professionals cannot provide documentation. In addition, recipients of EHR incentive payments should be sure that they have conducted and documented a data security risk analysis that reviews the potential risks and vulnerabilities to the confidentiality, integrity, and availability of their electronic protected health information in accordance with the requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). As noted in the OIG report, such risk analyses are required to establish meaningful use, and auditors will request documentation of a risk analysis in an audit.

Eligible professionals who have reason to believe that they previously received EHR incentive payments without meeting meaningful use objectives should also consider whether they are obligated to report and return such payments pursuant to the Medicare Part A and B overpayment rule. While CMS’s refusal to adopt OIG’s recommendation to take further action to recover overpayments made under the EHR incentive program signals that the government may not aggressively pursue reverse FCA claims related to the retention of EHR incentive program overpayments, providers should be cognizant of the potential for such claims if overpayments are identified through an audit or by a whistleblower.