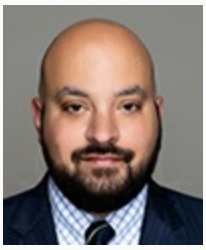
COSMOS
Navigate the Compliance Universe

Compliance Today - July 2022
The government giveth and the government taketh away: Government enforcement and electronic health records


Scott R. Grubman

By Scott R. Grubman

Scott R. Grubman (sgrubman@cglawfirm.com) is a partner at Chilivis Grubman in Atlanta, Georgia, where he focuses his practice on representing healthcare providers of all types and sizes in connection with government investigations and False Claims Act litigation.

- linkedin.com/in/sgrubman/

In 2011, the Centers for Medicare & Medicaid Services (CMS) established the Medicare and Medicaid EHR Incentive Programs—now known as the Medicare Promoting Interoperability Program—to encourage healthcare providers to "adopt, implement, upgrade, and demonstrate meaningful use of certified electronic health record technology."[1] Then, in 2016, CMS announced that it had allocated nearly $35 billion in meaningful use incentive payments to more than 500,000 providers.[2]

As with most well-intentioned, government-backed incentive programs, outlay of those funds has been followed by years of scrutiny and government enforcement actions. In June 2017, the U.S. Department of Health & Human Services (HHS) Office of Inspector General (OIG) announced the findings of an audit alleging that CMS inappropriately paid more than $729 million in incentive payments to healthcare providers who did not meet meaningful use requirements.[3] In December 2019, OIG announced that, out of the $10.8 billion that went to acute-care hospitals, an estimated $93.6 million was incorrectly paid.[4]

It is not surprising then that the Department of Justice (DOJ) has dedicated significant resources to investigating and prosecuting fraud matters related to electronic health record (EHR) incentive payments and other aspects of the EHR industry. In December 2020, Deputy Assistant Attorney General Michael Granston, who oversees False Claims Act (FCA) enforcement, made remarks to the American Bar Association's Civil False Claims Act and Qui Tam Enforcement Institute.[5] Discussing the DOJ's FCA enforcement priorities, Granston identified fraud pertaining to EHRs as a likely "focal point" of the DOJ's future enforcement efforts. According to Granston, "providers increasingly rely on electronic health records to provide vital and unbiased information to improve treatment outcomes for patients. While electronic software is intended to reduce errors and improve the delivery of care, the transition to a digital format has also introduced new opportunities for fraud and abuse."

Enforcement actions against EHR vendors

Almost two months prior to Granston's remarks, the DOJ announced a proposed settlement with opioid manufacturer Purdue Pharma, wherein Purdue and individual shareholders agreed to pay more than $8 billion to resolve various criminal and civil fraud allegations regarding its marketing of OxyContin and other opioid products.[6] Part of that settlement involved allegations that Purdue paid EHR vendor Practice Fusion in exchange for recommending Purdue's opioid products. In January 2020, Practice Fusion agreed to pay $145 million to resolve criminal and civil kickback allegations involving the same arrangement.[7] As part of that

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

settlement, Practice Fusion admitted that it received kickbacks from Purdue "in exchange for utilizing its EHR software to influence physician prescribing of opioid pain medications." Specifically, Practice Fusion set up "clinical decision support" alerts in its EHR system, where the EHR system alerted the provider-user when certain criteria were met that would make it appropriate to prescribe the opioid. According to the government's allegations, Practice Fusion allowed pharmaceutical companies to participate in the designing of those alerts, "including selecting the guidelines used to develop the alerts, setting the criteria that would determine when a healthcare provider received an alert, and in some cases, even drafting the language used in the alert itself."

This was not the first time that the DOJ brought a fraud enforcement action against an EHR vendor. For example, in May 2017, it announced that EHR vendor eClinicalWorks (ECW) agreed to pay $155 million to resolve allegations that it violated the FCA by paying kickbacks to certain customers in exchange for promoting its product.[8] The government also alleged that ECW obtained a "meaningful use" certification by concealing that its software failed to comply with certain requirements for such certification. According to the government, this false certification by ECW in turn caused healthcare providers who used the EHR program to submit false claims for meaningful use incentive payments.

Nearly two years later, in February 2019, the DOJ announced another large settlement against EHR vendor Greenway Health, which agreed to pay more than $57 million to resolve FCA allegations.[9] Similar to the allegations in the ECW case, the DOJ alleged that Greenway misrepresented the capabilities of its EHR product, thereby causing its users to submit false claims for meaningful use incentive payments. The following year, EHR vendor Konica Minolta Healthcare agreed to pay $500,000 to resolve similar FCA allegations involving false statements to the meaningful use incentive payment certification authority.[10]

Just a little over a month after Granston's remarks at the American Bar Association conference, in January 2021, the DOJ announced yet another FCA settlement with an EHR vendor, this time athenahealth Inc. (Athena). In this case, the DOJ alleged that Athena violated the FCA and the Anti-Kickback Statute by paying unlawful kickbacks to generate sales of its EHR product.[11] Specifically, the government alleged that Athena violated the law by inviting prospective and existing customers to "Concierge Events," providing free tickets and travel to sporting and entertainment events, as well as luxury accommodations, meals, and alcohol. The government also alleged that Athena paid kickbacks to its existing customers designed to identify and refer perspective clients. Three months later, in April 2021, the DOJ announced a $3.8 million settlement with EHR developer CareCloud Health, alleging that it offered and provided its clients with cash payments and bonuses to recommend its EHR product to perspective clients.[12]

A recent filing by the DOJ in Vermont suggests that the DOJ's enforcement against EHR vendors continue. On March 15, 2022, the DOJ filed a notice to intervene in an FCA qui tam action filed against EHR vendor Modernizing Medicine and several related individuals.[13] According to the relator's complaint in that case, Modernizing Medicine violated the FCA by allegedly misrepresenting its compliance with meaningful use requirements, providing certain remuneration to its users, and programming its EHR software in a way that resulted in "upcoding" of evaluation and management (E/M) codes and use of improper modifiers.

Enforcement actions against providers and individuals

EHR vendors were not alone in facing DOJ enforcement actions. In January 2019, pathology laboratory Inform Diagnostics agreed to pay $63.5 million to resolve allegations that it violated the FCA, Anti-Kickback Statute, and the Stark Law by providing to referring physicians EHR systems and free and discounted technology consulting services.[14] In May 2019, Coffey Health System, a small critical-access hospital in Kansas, agreed to pay $250,000 to resolve allegations that it violated the FCA by falsely certifying its meaningful use of its EHR

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

technology.[15] Specifically, the DOJ alleged that the hospital "falsely attested that it conducted and/or reviewed security risk analyses" in accordance with the requirements of the meaningful use incentive program.

There is at least one example of a criminal prosecution against an individual related to the EHR incentive program. In November 2014, Joe White, the former chief financial officer of Shelby County Hospital in Texas, pleaded guilty to making a false statement to Medicare, falsely representing that the hospital complied with meaningful use criteria.[16] The government alleged that, as a result of White's false statement, the hospital received over $785,655 from Medicare. White was eventually sentenced to 23 months in prison.

Risks to providers moving forward

As demonstrated by the cases discussed earlier, both EHR vendors and users face scrutiny and potential liability related to EHR software. Apart from potential liability related to false or fraudulent meaningful use certifications, providers that use EHR should be aware of other potential fraud-related landmines. CMS has noted that "while EHRs can improve health care delivery and provider services, they can pose provider challenges… [including] privacy and security, author identification, altering entry dates, cloning, upcoding, and coding modifiers."[17] In fact, from the early days of EHR technology, the government has flagged potential fraud and abuse concerns related to EHR. A September 2012 joint letter from then-HHS Secretary Kathleen Sebelius and Attorney General Eric Holder to the leaders of various healthcare industry groups warned that "there are troubling indications that some providers are using this [EHR] technology to game the system, possibly to obtain payments to which they are not entitled. False documentation of care is not just bad patient care; its illegal."[18] In December 2013, OIG issued a report in which it stated that "experts in health information technology caution that EHR technology can make it easier to commit fraud."[19]

The following are some examples of such potential issues.

Overreliance on EHR templates

The use of EHR templates is not, in and of itself, unlawful. In fact, the *Medicare Program Integrity Manual* expressly provides that CMS "does not prohibit the use of templates to facilitate record-keeping."[20] The *Medicare Program Integrity Manual* goes on to state, however, that CMS "discourages" the use of templates that overutilize check boxes, predefined answers, or limited space to enter information, as those templates "often fail to capture sufficient detailed clinical information to demonstrate that all coverage and coding requirements are met." The *Medicare Program Integrity Manual* also provides that providers 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."

While the use of templates is not illegal, overreliance on such templates is fraught with peril and often becomes the focus of government enforcement actions. One Medicare contractor—Noridian—notes that:

> In order for a claim for Medicare benefits to be valid, there must be sufficient documentation in the provider's or hospital's records to verify the services performed were 'reasonable and necessary' and required the level of care billed. If there is no or insufficient documentation, then there is no justification for the services or level of care billed. Additionally, if there is insufficient documentation on the claims that have already been adjudicated by Medicare, reimbursement may be considered an overpayment and the funds can be partially or fully recovered.[21]

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

While providers should feel comfortable relying on basic EHR templates designed to ease the process of capturing the relevant information regarding an encounter, providers should make sure that they are actually typing the relevant information (including, at minimum, the reason for the encounter, relevant history, findings, test results, date of service, assessment and impression of diagnosis, plan of care, and identity of the rendering provider) and not overrelying on prefilled boxes and drop-down menus.

Cloned notes

According to CMS, record "cloning" involves "copying and pasting previously recorded information from a prior note into a new note."[22] Similar to the use of templates, there is nothing inherently improper with cloning. As CMS itself recognizes "features like auto-fill and auto-prompts can facilitate and improve provider documentation, but they can also be misused." Cloning of medical records has long been identified as a potential area for abuse. The joint letter from the HHS secretary and attorney general from September 2012 specifically mentions cloning as an issue.[23] The December 2013 OIG report states that when healthcare providers use cloned records, "inaccurate information may enter the patient's medical record and inappropriate charges may be billed to patients and third-party health care payers. Furthermore, inappropriate copy-pasting could facilitate attempts to inflate claims and duplicate or create fraudulent claims."[24]

While providers may permissibly copy and paste certain information from a previous encounter that has not changed, they should do so only after confirming with the patient that the information remains accurate and has not changed. A provider would be well advised to expressly note in the documentation that all of the information was confirmed.

Reliance on EHR coding algorithms

Many EHR systems include a feature that uses an algorithm that assists the provider in selecting the proper billing code—particularly E/M codes. For example, one such EHR system (which will remain unnamed to protect the allegedly innocent) advertises on its website that its "comprehensive E&M calculator generates accurate codes for you. This tool helps prevent undercoding and maximizes reimbursement for the services you provide."

As with previously mentioned cases, while there is nothing inherently illegal or improper with using E/M calculators or other code-selection algorithms, it is important to remember that it is the provider whose signature and national provider identifier are on the claim who is ultimately responsible for the accuracy of the coding. While a provider should feel free to use the technology to *assist* in choosing the correct code, the provider should also do their own analysis to ensure accurate coding.

Audit logs

Most, if not all, EHR systems contain "audit trails" or "audit logs." In fact, in order to qualify for meaningful use, an EHR must maintain an audit log adhering to certain requirements.[25] Audit logs can be useful to providers under certain circumstances. For example, where there is an allegation of unauthorized access to protected health information, the provider can use its EHR audit logs to determine whether any such unauthorized access occurred and, if so, the details.

Perhaps more often, however, audit logs provide an opportunity for auditors and investigators to uncover evidence of potential wrongdoing or fraud. For example, where a healthcare provider attempts to add information to a patient's medical record after receiving a request for additional documentation, the auditor/investigator will be able to use the logs to determine what information was added and when. This could

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

support an allegation that the provider was attempting to obstruct an audit or provide falsified documentation to the auditor. While there is really nothing that a provider can do about this, it is enough for providers to understand that each and every log-in and keystroke may be, and probably is, recorded for prosperity's sake, and that investigators often request such information as part of fraud investigators.

Conclusion

Like other modern technology, EHR provides both opportunity and risk to healthcare providers. On the one hand, EHR software has and continues to provide cost-efficient opportunities for providers to improve medical documentation and communicate with their patients. On the other hand, EHR technology brings with it much risk from an enforcement perspective, particularly where providers become overly reliant on the technology. While healthcare providers should feel free to use their EHR systems and all of the features included therein, providers should remember that, ultimately, the accuracy of their documentation and claims for reimbursement are their responsibility, and reliance on EHR technology might not be a sufficient defense to an enforcement action. Providers must also remember that receiving payments from EHR vendors could implicate the Anti-Kickback Statute and ensure that all such payments are compliant.

Takeaways

- In the 11 years since it announced its meaningful use incentive program, the Centers for Medicare & Medicaid Services has paid healthcare providers billions of dollars in incentive payments.
- Government auditors estimate that nearly a billion dollars of incentive payments were improperly paid, leading to a barrage of government audits and investigations.
- Electronic health record (EHR) vendors have paid millions of dollars to resolve allegations that they violated the False Claims Act and Anti-Kickback Statute based on both their relationships with their provider-users, as well as their compliance with meaningful use regulations.
- Healthcare providers have also faced significant scrutiny related to their use of EHR systems, paying millions of dollars in False Claims Act settlements.
- While EHR technology continues to assist healthcare providers in maintaining compliant documentation and effectively communicating with their patients, overreliance on the technology could result in government scrutiny or even liability. Providers should be careful not to overly rely on such technology and ensure compliance in their relationship with the EHR vendor.

1 "Promoting Interoperability Programs," Centers for Medicare & Medicaid Services, last modified April 25, 2022, https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms.
2 Centers for Medicare & Medicaid Services, "EHR Incentive Program," summary report, May 2016, https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/May2016_SummaryReport.pdf.
3 U.S. Department of Health & Human Services, Office of Inspector General, "Medicare Paid Hundreds of Millions in Electronic Health Record Incentive Payments That Did Not Comply With Federal Requirements," June 7, 2017, https://oig.hhs.gov/oas/reports/region5/51400047.asp.
4 Joanne M. Chiedi, *CMS Made an Estimated $93.6 Million in Incorrect Medicare Electronic Health Record Incentive Payments To Acute-Care Hospitals, or Less Than 1 Percent of $10.8 Billion in Total Incentive Payments*, A-09-18-03020, Office of Inspector General, U.S. Department of Health & Human Services, December 2019, https://oig.hhs.gov/oas/reports/region9/91803020.pdf.

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

5 U.S. Department of Justice, "Remarks of Deputy Assistant Attorney General Michael D. Granston at the ABA Civil False Claims Act and Qui Tam Enforcement Institute," December 2, 2020, https://www.justice.gov/opa/speech/remarks-deputy-assistant-attorney-general-michael-d-granston-aba-civil-false-claims-act.
6 U.S. Department of Justice, "Justice Department Announces Global Resolution of Criminal and Civil Investigations with Opioid Manufacturer Purdue Pharma and Civil Settlement with Members of the Sackler Family," news release, October 21, 2020, https://www.justice.gov/opa/pr/justice-department-announces-global-resolution-criminal-and-civil-investigations-opioid.
7 U.S. Department of Justice, "Electronic Health Records Vendor to Pay $145 Million to Resolve Criminal and Civil Investigations," news release, January 27, 2020, https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-145-million-resolve-criminal-and-civil-investigations-0.
8 U.S. Department of Justice, "Electronic Health Records Vendor to Pay $155 Million to Settle False Claims Act Allegations," news release, May 31, 2017, https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-155-million-settle-false-claims-act-allegations.
9 U.S. Department of Justice, "Electronic Health Records Vendor to Pay $57.25 Million to Settle False Claims Act Allegations," news release, February 6, 2019, https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-5725-million-settle-false-claims-act-allegations.
10 U.S. Department of Justice, U.S. Attorney's Office for the District of New Jersey, "New Jersey Electronic Health Records Company to Pay $500,000 to Resolve False Claims Act Allegations," news release, August 27, 2020, https://www.justice.gov/usao-nj/pr/new-jersey-electronic-health-records-company-pay-500000-resolve-false-claims-act.
11 U.S. Department of Justice, "Electronic Health Records Technology Vendor to Pay $18.25 Million to Resolve Kickback Allegations," news release, January 28, 2021, https://www.justice.gov/opa/pr/electronic-health-records-technology-vendor-pay-1825-million-resolve-kickback-allegations.
12 U.S. Department of Justice, U.S. Attorney's Office for the Southern District of Florida, "Miami-Based CareCloud Health, Inc. Agrees to Pay $3.8 Million to Resolve Allegations that it Paid Illegal Kickbacks," news release, April 30, 2021, https://www.justice.gov/usao-sdfl/pr/miami-based-carecloud-health-inc-agrees-pay-38-million-resolve-allegations-it-paid.
13 *See* U.S. ex rel. Long v. Modernizing Medicine, Inc. et al., No. 2:17-cv-179 (D. Vt.) (March 15, 2022).
14 U.S. Department of Justice, "Pathology Laboratory Agrees to Pay $63.5 Million for Providing Illegal Inducements to Referring Physicians," news release, January 30, 2019, https://bit.ly/3L6sMJQ.
15 U.S. Department of Justice, U.S. Attorney's Office for the District of Kansas, "Kansas Hospital Agrees to Pay $250,000 To Settle False Claims Act Allegations," news release, May 31, 2019, https://www.justice.gov/usao-ks/pr/kansas-hospital-agrees-pay-250000-settle-false-claims-act-allegations.
16 U.S. Department of Justice, U.S. Attorney's Office for the Eastern District of Texas, "Former Shelby County Hospital CFO Sentenced in EHR Incentive Case," news release, June 17, 2015, https://www.justice.gov/usao-edtx/pr/former-shelby-county-hospital-cfo-sentenced-ehr-incentive-case.
17 Centers for Medicare & Medicaid Services, "Electronic Health Records Provider Fact Sheet," December 2015, https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/Downloads/docmatters-ehr-providerfactsheet.pdf.
18 Kathleen Sebelius and Eric H. Holder, Jr., letter to chief executive officers, September 24, 2012, https://www.modernhealthcare.com/Assets/pdf/CH82990924.PDF.
19 Daniel R. Levinson, *Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology*, OEI-01-11-00570, Office of Inspector General, U.S. Department of Health & Human Services, December 2013, https://oig.hhs.gov/oei/reports/oei-01-11-00570.pdf.
20 Centers for Medicare & Medicaid Services, "Chapter 3 - Verifying Potential Errors and Taking Corrective Actions," § 3.3.2.1.1, *Medicare Program Integrity Manual*, Pub. 100-08, revised September 30, 2021,

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/downloads/pim83c03.pdf.
21 "Documentation Guidelines for Medicare Services," Medical Review, Jurisdiction E - Medicare Part B, Noridian Healthcare Solutions, last updated January 2, 2020, https://med.noridianmedicare.com/web/jfb/cert-reviews/mr/documentation-guidelines-for-medicare-services.
22 Centers for Medicare & Medicaid Services, "Electronic Health Records Provider Fact Sheet."
23 Sebelius, letter to chief executive officers.
24 Daniel R. Levinson, *Not All Recommended Fraud Safeguards Have Been Implemented*.
25 Centers for Medicare & Medicaid Services, "Eligible Professional Meaningful Use Core Measures, Measure 9 of 17, Stage 2," last updated November 2014, https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/Stage2_EPCore_9_ProtectElectronicHealthInfo.pdf.

This publication is only available to members. To view all documents, please log in or become a member.

Become a Member Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.