

Congratulations, John!

Winner of the Compliance Institute's
"#HCCAcI" Twitter contest for 2014

an interview with John H. Fisher, II
Health Care Attorney, Ruder Ware

See page 16



27

**Pitfalls and risks
underlying the EHR
incentive programs**

Alexis Gilroy, Kristen McDonald,
Robert Sherman, and
Matthew Bowles

33

**Mobile devices
and medical apps
in the healthcare
workplace**

Theresamarie Mantese and
John R. Wright

43

**The mistake
and reality of
one-size-fits-all
compliance
management**

Brian Santo

49

**The art of
communication
and the
compliance
message**

Bret S. Bissey

by Alexis Gilroy, Kristen McDonald, Robert Sherman, and Matthew Bowles

Pitfalls and risks underlying the EHR incentive programs

- » Understand risks associated with preparing and submitting EHR attestations.
- » Negotiate EHR contracts that enable upgrades and risk-sharing.
- » Perform ongoing due diligence of EHR vendors.
- » Develop procedures, train key personnel, and hold mock audits.
- » Consider engaging counsel for privilege protection purposes.

Alexis Gilroy (agilroy@jonesday.com) and **Kristen McDonald** (kmcdonald@jonesday.com) are Partners at Jones Day and **Robert Sherman** (resherman@jonesday.com) and **Matthew Bowles** (mbowles@jonesday.com) are associates at the firm.

To date, more than 90% of hospitals and health systems have adopted information technology tools like electronic health records (EHRs) and other care management systems. This is due, in large part, to Medicare and Medicaid programs providing



Gilroy

incentive payments for eligible providers that attest to the “meaningful use” of such technologies.¹ Given the more than \$22 billion in EHR incentives distributed since 2011, providers receiving incentive payments should evaluate possible risks of increased regulatory oversight, as well as financial and legal liability, if EHR attestations prove inaccurate or unsubstantiated, or if the ongoing utilization of the technologies fails to meet program objectives.



McDonald

In light of these concerns, now is the time for providers to evaluate various mitigation strategies for managing such risks, chief among them are the following: (1) negotiate indemnification and other risk-sharing provisions

in information technology vendor contracts; (2) perform ongoing due diligence of EHR vendors; (3) update pertinent policies and procedures, train key personnel, and perform mock audits of meaningful use attestations; and (4) consider engaging counsel for privilege protection purposes.



Sherman

Meaningful use to date and the path ahead

Pursuant to the HITECH Act of 2009, Medicare and Medicaid provide financial incentives to eligible hospitals and healthcare professionals that adopt, implement, and demonstrate they are using certified EHR technologies to advance positive health outcomes consistent with certain identified meaningful uses (referred to as EHR Incentive Programs).²

The EHR Incentive Programs involve three stages in which participants must demonstrate increasing levels of compliance with core objectives and menu objectives. Core objectives focus on foundational elements for advancing healthcare efficiency and quality, such as electronic prescribing, clinical decision support, and protection of health information. Participants also must attest to satisfying select menu objectives, such as drug formulary



Bowles

checks and patient-specific education. For Stage 1, participants must meet 18 of 22 objectives for demonstration of meaningful use and, thus qualify for the incentive payments. Participants must satisfy these Stage 1 criteria before advancing to Stage 2, which, among other things, raises the number of core objectives and places greater emphasis on achieving interoperability among EHR systems. The Centers for Medicare & Medicaid Services (CMS) has yet to promulgate requirements for Stage 3.

In response to the EHR Incentive Programs, there has been widespread adoption of EHR technology, with more than 90% of eligible hospitals and nearly 70% of eligible professionals having received payments for implementing certified technology—a five-fold increase since 2008 for non-federal acute care hospitals.³ On October 1, 2013, hospitals achieving Stage 1 meaningful use objectives for two or more years began advancing to the next round of attestation. These hospitals must now demonstrate they meet Stage 2 requirements for a 90-day period before the end of the government fiscal year (September 30, 2014), and as of May 6, 2014, only four have reported doing so. Meanwhile, participating professionals—whose programs follow a calendar year—have until the end of 2014 to solidify Stage 2 attestations.⁴

Understandably, incentive payments are just one of the policy tools available to regulators for the promotion of EHR technologies and the ultimate exchange of healthcare information for more efficient and effective healthcare services. Another effective policy tool is the reduction of Medicare

reimbursement for those eligible healthcare providers failing to achieve core and menu objectives (i.e., meaningful use of certified EHRs) by a specific date. For example, beginning in October 2014, hospitals not meeting the objectives will be subject to a negative payment adjustment of 25% to the standard update for their annual inpatient payments from Medicare. In fact, beginning in 2015, eligible professionals that fail to demonstrate meaningful use will face a 1% reduction in their Physician Fee Schedule reimbursement. The penalty

could increase to as much as 5% by 2019 if fewer than three-fourths of professionals comply with the EHR Incentive Programs.⁵

Potential liabilities for non-compliance

By participating in EHR Incentive Programs and making attestations of meaningful use, eligible providers and professionals may face new and uncertain liabilities. As discussed more fully below, the most immediate risk is that of audits conducted by federal and state contractors on behalf of the Medicare and Medicaid programs. Because meaningful use is an all-or-nothing proposition in terms of meeting all requirements or risking the loss of incentive payments, an audit with negative findings may subject the provider to recoupment of the entire incentive payment. Another looming risk is the potential for enforcement actions brought by the government under fraud and abuse laws, such as the federal False Claims Act (FCA) or state equivalents, which may lead to potential civil penalties and damages, or possible criminal enforcement.

...more than 90% of eligible hospitals and nearly 70% of eligible professionals [have] received payments for implementing certified technology—a five-fold increase since 2008...

Meaningful use audits

Hospitals and professionals should be prepared for meaningful use audits and the risk of potential recoupment of EHR incentive payments. At the federal level, CMS has indicated that it expects to audit approximately 5%–10% of providers that have received payments under EHR Incentive Programs.⁶ Once again, if the government auditor determines that any aspect of the attestation requirements is unmet, the provider may be at risk of receiving a demand for recoupment of an incentive payment.

Though it is relatively early in the life of the EHR Incentive Programs, some risk patterns have emerged in meaningful use audits. One main risk is a provider's untimely response, particularly in light of the two-week deadline in which providers are required to respond to document requests from government auditors. A second concern involves failing to maintain documentation supporting the meaningful use attestations. Audits are also flagging the perceived failure of providers to conduct adequate security risk assessments of EHR system vulnerabilities.⁷

It may be wise for providers to consider taking certain immediate steps to ensure readiness for meaningful use audits. Initially, providers should designate a person (or a committee, in the case of large entities) to oversee meaningful use matters. CMS guidance specifically advises hospitals and professionals to maintain supporting documentation of meaningful use objectives and clinical quality measures for at least six years post-attestation. It is important to note that an EHR system must be certified for the entire attestation period. Merely upgrading an EHR system to a certified version prior to the close of the attestation period is not sufficient because CMS requires that all clinical quality data come directly from a certified system. It is also wise to ensure that all supporting data is readily available and organized in a manner to

enable timely responses to auditor document requests. Heightened preparation will assist in an effective defense of meaningful use attestation audits.⁸

Potential civil liability under the FCA

In addition to the risk of potential audits, another concern involving meaningful use attestations is a government investigation under the FCA. By way of background, liability under the FCA may attach to a provider who “knowingly presents, or causes to be presented, a false or fraudulent claim for payment” to the federal government.⁹ Liability can also attach for conspiracy to make false claims; for causing third parties to make false claims; and for improperly concealing, avoiding, or decreasing a payment obligation to the federal government (also known as a reverse false claim). The term “knowingly” includes actual knowledge, deliberate ignorance, or reckless disregard. Claims under the FCA are subject to treble damages (i.e., three times the damages amount calculated from the reimbursement amount per claim), in addition to civil penalties ranging from \$5,500 to \$11,000 for each false claim.

Of specific relevance to EHR attestations is the risk that the government may assert a false certification theory of liability, in which a provider “knowingly falsely certifies that it has complied with a statute or regulation the compliance with which is a condition for government payment.”¹⁰ In other words, for a false certification theory of liability, there must be a certification of compliance with a statute or regulation that is a condition of payment as compared to a condition of participation. There is a wide breadth of case law evaluating conditions of payment versus conditions of participation, as well as the scope of a false certification theory of liability, including effective defenses. The fact remains that the current environment has seen an uptick

in government enforcement actions. Thus, it may be simply a matter of time before the government increases its scrutiny of attestations using other avenues beyond audits.

Potential criminal liability under the FCA

It is also important to note the risk of potential criminal liability involving meaningful use attestations. Indeed, executives falsely attesting to meaningful use of EHR technology may face criminal penalties in addition to civil enforcement actions. For example, on January 22, 2014, the chief financial officer of a hospital system was indicted on federal charges stemming from alleged false claims made pursuant to attestations regarding meaningful use.¹¹ This is a recent and singular case, but this example clearly demonstrates the federal government's willingness to pursue criminal actions in certain instances. Accordingly, the utmost care should be made in monitoring and documenting a provider's meaningful use requirements.

Mitigation strategies to consider

Fortunately, with advanced preparation and participation, employees, hospitals, and professionals may be able to reduce the foregoing risks by taking some or all of the following actions.

Know your EHR agreement and consider risk-sharing strategies with your vendor

It is important that hospitals and professionals fully understand their rights, as well as EHR vendors' representations and obligations in vendor agreements. In particular, as providers rely on the appropriate certification of such technology and the continued functionality of the technology, they may want to consider negotiating specific representations and ongoing covenants appropriate to ensure the equipment and software they are purchasing complies with basic requirements and allows for potential future upgrades. Further, providers would be wise to consider indemnification and other risk-sharing contractual arrangements in the event the technical

aspects of the EHR result in flawed reports underlying attestations or the EHR is decertified by the Office of the National Coordinator for Health Information Technology (ONC) after entering into the contract.

For example, providers making attestations must utilize EHR systems that meet the latest functional standards of the EHR Incentive Programs. In May, CMS and ONC announced a proposed rule to give hospitals and providers more flexibility in this area—at least for the current year. Under the proposal, participants attesting to

meaningful use this year must meet either the 2011 edition technical standards or a combination of those standards and the more recent

It is also important to note the risk of potential criminal liability involving meaningful use attestations.

Indeed, executives falsely attesting to meaningful use of EHR technology may face criminal penalties in addition to civil enforcement actions.

2014 edition.¹² Also, earlier this year, ONC initiated a rulemaking to begin developing the next set of software standards for 2015. These actions demonstrate regulators' interest in continually promoting incremental improvements, including changes that could impact audits. For this reason, contracts with vendors should provide for ease of software upgrades to keep up with ever-changing technical requirements.

Perform ongoing due diligence of EHR vendors

As noted above, the ONC is responsible for certifying EHR products and, through continued monitoring, also decertifies products upon discovering problems with the technology. In light of this, providers should perform upfront and ongoing diligence of their EHR technology and even consider monitoring the ONC website to catch any decertification announcements regarding vendor EHR technology.

Develop policies and procedures, train employees, and conduct mock audits
Adequate training and preparation are other mitigation strategies. Some providers fall into the trap of developing an EHR system that is certified to meet various meaningful use criteria but is not used in daily practice. These particular providers may instead continue to rely on earlier, uncertified systems. Because the purpose of the EHR Incentive Programs is to integrate technology that improves patient outcomes and the exchange of information, auditors most likely will review whether the certified EHR is being used for that purpose. Training employees in new systems, developing standard procedures, and routinely monitoring these policies can reduce the risks inherent with failures to meet meaningful use standards.

In addition, it may be wise for providers to create audit preparation teams with key leaders to oversee data collection and

management. Mock audits may also be helpful to make sure employees are well-versed in how to respond if an audit is initiated.

Consider engaging counsel for privilege protection purposes

As a final matter, hospitals and professionals may want to consider engaging legal counsel to assist with developing audit preparation strategies so as to ensure that such strategies are protected by the attorney-client privilege. Furthermore, if consultants on meaningful use are considered, it may be wise to engage such consultants through counsel, once again, to ensure the protections of the attorney-client privilege.

Summary

Eligible providers should develop comprehensive strategies to demonstrate appropriate ongoing EHR meaningful use and to substantiate related attestations so they can reduce the risks of negative audit findings, potential recoupment of EHR incentive payments, and other government enforcement actions that may otherwise surface. ☐

1. Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111-5, 123 Stat. 226 (codified at 42 U.S.C. 201 et seq.)
2. CMS website: EHR Incentive Programs. Available at go.cms.gov/1r5ZNID
3. Dustin Charles, Meghan Gabriel, Michael Furukawa: ONC Data Brief No. 16, Adoption of Electronic Health Record Systems Among U.S. Non-Federal Acute Care Hospitals: 2008-2013. May 2014. Available at <http://bit.ly/1sxKhFj>
4. Joseph Conn: "Few Hospitals, Docs at Stage 2 Meaningful Use, CMS Official Says," Modern Healthcare, May 6, 2014. Available at <http://bit.ly/1tjwyWP>
5. 42 C.F.R. § 495.102 et seq. – Incentive payments to EPs, eligible hospitals
6. Frank Irving: "CMS Official Offers Details on MU Audits," Healthcare IT News, May 3, 2013. Available at <http://bit.ly/1zmQk4f>
7. ONC: Guide to Privacy and Security of Health Information. Available at <http://bit.ly/U1elxd>
8. CMS: EHR Incentive Programs Supporting Documentation for Audits. February 2013. Available at <http://go.cms.gov/1n43WHN>
9. False Claims Act: 31 U.S.C. § 3279(a)(1)(A). The knowledge standard and penalty framework are defined respectively at id. § 3279(b)(1) and id. § 3279(a) (as updated for inflation)
10. *United States ex. rel. Wilkins v. UnitedHealth Group, Inc.* 659 F.3d 295, 305, 309 (3d. Cir. 2011)
11. Federal Bureau of Investigation, press release: "Former Hospital CFO Charged with Health Care Fraud." February 6, 2014. Available at <http://1.usa.gov/1r61Hsy>
12. CMS: Modifications to the Medicare and Medicaid Electronic Health Record Incentive Programs for 2014; and Health Information Technology: Revisions to the Certified EHR Technology Definition, 79 Fed. Reg. 29,732 (proposed May 23, 2014). Available at <http://1.usa.gov/1xMHnQ7>