ELECTRONIC HEALTH RECORDS: REGULATORY RISKS AND COMPLIANCE ISSUES

Felicia E. Heimer
Senior Counsel, Office of Counsel to the Inspector General, U.S. Department of Health and Human Services

James A. Cannatti III
Partner, McDermott Will & Emery

HCCA 25th Annual Compliance Institute

April 21, 2021

mwe.com

McDermott Will & Emery

1

FELICIA E. HEIMER

Senior Counsel
felicia.heimer@oig.hhs.gov

Felicia Heimer is a senior attorney with the Office of Inspector General of the United States Department of Health and Human Services where she represents the agency on a wide range of health care fraud and compliance matters including the settlement of cases arising under the False Claims Act, the resolution of matters under the Self-Disclosure Protocol, and the negotiation and monitoring of Corporate Integrity Agreements. Prior to entering government service, Ms. Heimer worked for a global litigation advisory firm assisting health systems, pharmaceutical manufacturers and their boards of directors in responding to government investigations and conducting internal compliance reviews. Ms. Heimer began her legal career at an academic medical center and research institute in Southern California.

2

2

JAMES A. CANNATTI III

Partner
Washington, DC
+1 202 756 8866 | jcannatti@mwe.com

CAPABILITIES

James practices at the intersection of today's most pertinent health care issues, including digital health, health IT policy, and fraud and abuse, including Anti-Kickback Statute/Stark Law matters. With more than 10 years of experience in the US Department of Health and Human Services' Office of Inspector General most recently as Senior Counselor for Health Information Technology, James is well-attuned to the regulatory issues impacting the rapidly evolving digital health landscape, including information blocking and interoperability, electronic health records, and value-based care.

3

AGENDA

- Background on EHR Incentive Programs / Promoting Interoperability
- Overview of the False Claims Act and Anti-Kickback Statute
- Recent EHR Developer Enforcement Trends
- Overview of OIG's Corporate Integrity Agreement Requirements for EHR Developers
- Examples of Quality and Compliance Risks
- Compliance Measures for EHR Developers and Software Users to Address Risks

4

EHR INCENTIVE PROGRAMS / PROMOTING INTEROPERABILITY

5

EHR INCENTIVE PROGRAMS / PROMOTING INTEROPERABILITY

- Congress authorized the Medicare and Medicaid EHR Incentive Programs as part of the HITECH Act in 2009
- EHR Incentive Programs provided payments to certain eligible professionals (EPs) and eligible hospitals (EHs) who achieved "Meaningful Use" of Certified EHR Technology (CEHRT) by meeting certain Meaningful Use measures
- Incentive payments paid to Medicare EPs and EHs until 2016
- Downward MPFS payment adjustments for failing to achieve Meaningful Use began in 2015

6

STEPS REQUIRED TO ACHIEVE MEANINGFUL USE

- Implement CEHRT certified by certifying body approved by the Office of the National Coordinator of Health IT (ONC)
  - "Complete EHR" or a collection of "EHR Modules"
- Achieve Meaningful Use in Applicable Reporting Period
- Report on Electronic Clinical Quality Measures (eCQMs)
- Submit Attestation of Meaningful Use to CMS

7

MERIT-BASED INCENTIVE PAYMENT SYSTEM (MIPS)

- MIPS consolidated Medicare requirements of three existing quality programs into one incentive program starting with the 2017 reporting year:
  - Physician Quality Reporting System (PQRS)
  - Value Based Payment Modifier (VBPM)
  - Meaningful Use (MU)

8

ONC HEALTH IT CERTIFICATION PROGRAM

- ONC establishes criteria for health IT vendors to meet in order to certify their health IT as Certified Health Information Technology
- Some Health IT Modules are ***required*** in order to implement a **Base EHR**.
- Health care provider may adopt Health IT Modules from different vendors to complete a Base EHR
- Other Health IT Modules (and certification criteria) are optional for a health care provider to implement
- Three major "editions" of certification criteria; current edition is 2015 Edition

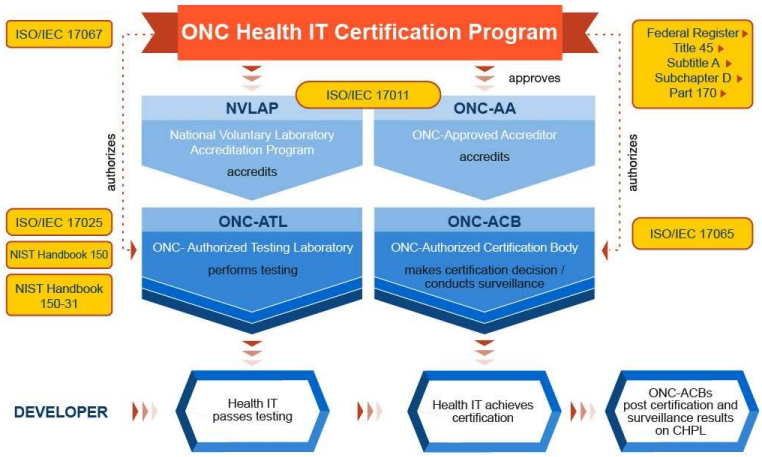
9

TESTING AND CERTIFICATION

- **Testing**
  - Health IT Modules must be tested by Authorized Testing Laboratory (ONC-ATL) for conformance with certification criteria, except for criteria where ONC permits self-attestation
  - ONC publishes test procedures on healthit.gov
  - If the Health IT Module passes testing for required certification criteria, then the Health IT Module may be referred to the vendor's Authorized Certification Body (ONC-ACB) for certification
- **Certification**
  - ONC-ACB determines based on testing results whether a Health IT Module may be certified and posts certification results on the Certified Health IT Product List
  - ONC-ACB receives complaints from users, conducts surveillance and determines whether a Health IT Module performs in the field as tested by ONC-ATL
  - ONC-ACB conducted randomized surveillance in the past, but ONC recently directed ONC-ACBs to focus on "reactive surveillance" (surveillance of complaints)
  - Vendors must report any changes made to the certified functionality of a Health IT Module to ONC-ACB

10

DIAGRAM OF ONC HEALTH IT CERTIFICATION PROGRAM



Source: https://www.healthit.gov/topic/certification-ehrs/about-onc-health-it-certification-program

11

OVERVIEW OF THE FALSE CLAIMS ACT AND ANTI-KICKBACK STATUTE

12

FALSE CLAIMS ACT (FCA)
31 U.S.C. § 3729-3733

- Prohibits knowingly presenting, or causing to be presented, a claim to the U.S. Government that is false or fraudulent
- Knowledge
  - Actual knowledge
  - Reckless disregard
  - Deliberate ignorance
- False or Fraudulent
  - Tainted by non-compliance with another law (*e.g.*, Anti-Kickback Statute)
  - Not medically necessary
  - Billed item or service is not the same as item or service provided

13

FCA (CONT)

Penalties

Treble Damages + $11,665-$23,331 per claim =

14

FCA (CONT)

- *Qui tam* actions are brought by private citizen whistleblowers (referred to as "relators") on behalf of the U.S. government
- Relator must be an original source (*i.e.*, something U.S. government has not learned from another source)
- Relator "Bounty" = 15 - 30% of the government's recovery
  - Relators also may assert anti-retaliation claims to obtain additional awards
  - Defendant pays the relator's attorneys' fees if settlement or judgment

15

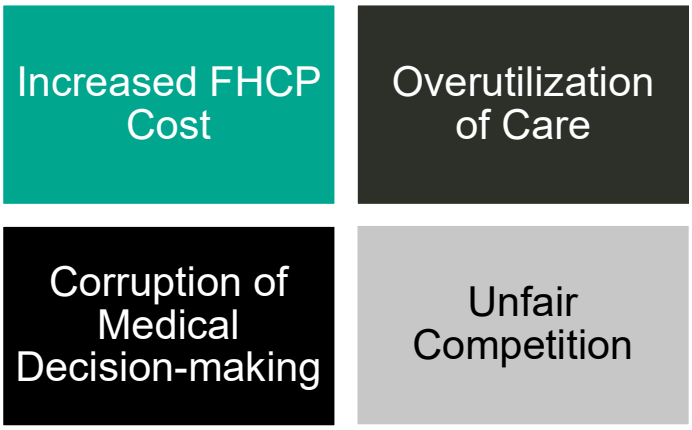
ANTI-KICKBACK STATUTE (AKS) 42 U.S.C. § 1320a-7b(b)

- AKS prohibits knowingly and willfully:
  - Offering, paying, soliciting, or receiving (by anyone, including non-providers)
  - Anything of value ("remuneration") (directly or indirectly, in cash or in kind)
  - In return for or to induce 1) referrals; 2) purchasing, leasing, ordering; or 3) arranging for or recommending purchasing, leasing, or ordering of
  - Items or services paid for, in whole or in part, by a FHCP
- "One purpose" test: outside safe harbors, if any one purpose is improper, other legitimate purposes may not carry the day

Bottom Line: No payments to induce referrals or purchases of FHCP items and services

16

AKS SEEKS TO PREVENT FOUR PROBLEMS



17

AKS: ENFORCEMENT PENALTIES

AKS enforcement exists in three forms	
Criminal	AKS is a criminal statute • Felony subject to up to $100,000 fine and ten years in prison
Civil	Civil prosecution under False Claims Act: • Up to 3 times damages and $22,363 penalty per claim • Settlements typically range 2-3 times damages • Corporate Integrity Agreement (CIA) with OIG
Administrative	• Civil money penalties of up to 3 times amount of kickback and $104,330 per kickback • Exclusion from participation in federal health care programs

18

AKS ENFORCEMENT ORGANIZATION

- HHS Office of Inspector General (OIG)
  - Creates regulatory safe harbors
  - Issues Advisory Opinions for specific arrangements
  - Issues industry guidance, such as bulletins, alerts, compliance program guidance
  - Advises DOJ on criminal and civil cases
  - Brings administrative CMPs and exclusion cases
  - Negotiates and monitors CIAs

19

AKS SAFE HARBORS

- Statutory and regulatory safe harbors protect certain arrangements even if intent is to induce referrals
- Must meet all elements
- Voluntary
- Narrowly drafted on purpose

20

AKS: OUTSIDE THE SAFE HARBORS

- Non-safe harbored arrangements analyzed based on specific facts and circumstances
- No bright lines because:
  - State-of-mind is important
  - Bad intent can negate good intent
  - Corporate intent is collective
  - Bad intent can be contagious
  - Intent is not always knowable without hindsight

21

RECENT EHR DEVELOPER ENFORCEMENT TRENDS

22

ECLINICALWORKS (ECW) SETTLEMENT (MAY 2017)

- *Qui tam* FCA case brought by a relator
- Allegations that eCW made material false statements and concealed material facts about the capabilities of its software in connection with the government's EHR certification process
- Also alleged that eCW paid purported kickbacks in connection with certain marketing arrangements (*i.e.*, a referral program, site visit program, and a reference program) with influential customers to induce them to recommend eCW's EHR software, in violation of the AKS
- $155 million settlement plus novel five-year Corporate Integrity Agreement (CIA) with OIG

GREENWAY HEALTH LLC (GREENWAY) SETTLEMENT (FEBRUARY 2019)

- DOJ initiated FCA case (no relator involved)
- Like eCW, Greenway faced allegations that its EHR system did not function in the way it represented it during the certification process
- Also allegations that Greenway provided some customers whose EHR software was improperly calculating certain measures (which providers are required to achieve to be eligible for incentive payments) with incorrect calculations in order to enable them to receive incentive payments
- Per DOJ, this allegedly caused some Greenway customers to submit false claims to HHS for payment under the Promoting Interoperability Program
- Similar to eCW, DOJ alleged that Greenway paid purported kickbacks in connection with certain marketing arrangements
- $57.25 million settlement plus an eCW-like CIA

PRACTICE FUSION SETTLEMENT AND DPA (JANUARY 2020)

- Civil:
  - Like eCW and Greenway, Practice Fusion faced allegations that its EHR system did not function in the way it represented it during the certification process
  - Per DOJ, this allegedly caused some customers to submit false claims for incentive payments in connection with the Promoting Interoperability Programs
  - AKS allegations differed from eCW and Greenway, instead focusing on arrangements with pharmaceutical manufacturers related to development and deployment of clinical decision support (CDS) tools
- Criminal: Focused on one particular CDS arrangement
- Resolution:
  - Settlement agreement to resolve the civil case and DPA to resolve criminal case
  - $145M settlement in total

ATHENAHEALTH, INC. (ATHENA) SETTLEMENT (JANUARY 2021)

- *Qui tam* FCA cases brought by relators
- No allegations that Athena's EHR system did not function in the way it represented it during the certification process
- FCA allegations predicated on purported kickbacks in connection with certain marketing arrangements (*i.e.*, trips for current / potential customers, client lead generation arrangements with current customers, and arrangements with health IT companies that decided to discontinue their health IT products to recommend that their customers transition to Athena products)
- $18.5 M settlement; no CIA

COMMON THEMES

- A focus on:
  - EHR certification program and the developer's underlying EHR functionality compliance; and
  - Marketing arrangements involving customers or potential customers

27

CORPORATE INTEGRITY AGREEMENTS

NEW REQUIREMENTS FOR EHR DEVELOPERS

28

"Electronic health records have the potential to improve the care provided to Medicare and Medicaid beneficiaries, but only if the information is accurate and accessible. Those who engage in fraud that undermines the goals of EHR or puts patients at risk can expect a thorough investigation and strong remedial measures such as those in the novel and innovative Corporate Integrity Agreement [for EHR Developers].

~ Phillip Coyne, Special Agent in Charge, HHS OIG, 2017 DOJ Press Release

29

29

NEW PROVISIONS AND OBLIGATIONS

- Patient Safety and Certification Reporting
- Quality Assurance Program
- EHR Usability and Patient Safety Teams
- Software Quality Oversight/Independent Review Organization

30

30

PATIENT SAFETY AND CERTIFICATION REPORTING

- Policies and procedures for timely and effective identification, notification, reporting and remediation
- Procedures for taking immediate corrective action if a patient safety issue is identified/discovered; immediate access to senior management to provide resources to correct the problem
- Prompt notification to customers and users of issues, including whether appropriate urgency is being given to patient safety issues
- Clear, conspicuous and comprehensive listing of issues on customer portal – including steps the company is taking and/or actions the customer must take to remediate
- Reporting to Compliance Officer, Compliance Committee, Software Quality Oversight/Independent Review Organization, and ONC-ACB

31

31

QUALITY ASSURANCE PROGRAM

- Proactive monitoring of information regarding potential software defects, usability problems and other issues that may present patient safety or certification issues
- Reviewing, tracking, and completing root causes analyses of potential and identified issues
- Developing action plans to fully address and remediate issues and associated risks to patient safety; timely and effective implementation and enforcement of action plans.
- Mitigating issues and associated risks to patient safety
- Coordination of activities across business divisions, teams, internal units
- Assessing compliance with relevant laws, statutes, regulations, directives

32

32

EHR USABILITY AND PATIENT SAFETY TEAMS

- Usability Team – at least one physician (MD/DO), one registered nurse, and one pharmacist, including other appropriate employees, customers/consultants
- Patient Safety Team – staff, including licensed clinicians (at least one physician and one pharmacist), with experience in clinical system safety and EHR implementation experience
- Collaborative effort to evaluate usability and patient safety issues – drawing from Compliance, Quality Assurance Departments and Oversight Review Organization

33

33

SOFTWARE QUALITY OVERSIGHT/INDEPENDENT REVIEW ORGANIZATION

- Performs assessment of the effectiveness, reliability, and thoroughness of:
  - internal quality control systems
  - company's ability to identify and address issues with software including patient safety and certification issues
  - adherence to software standards and practices and CIA requirements
  - other quality assurance activities
- Performs assessment of systems to ensure that patient safety, certification and other issues are timely and effectively identified and remediated
- Performs assessment of company's ability to conduct root cause analyses of identified issues and to execute action plans to fully remediate issues

34

34

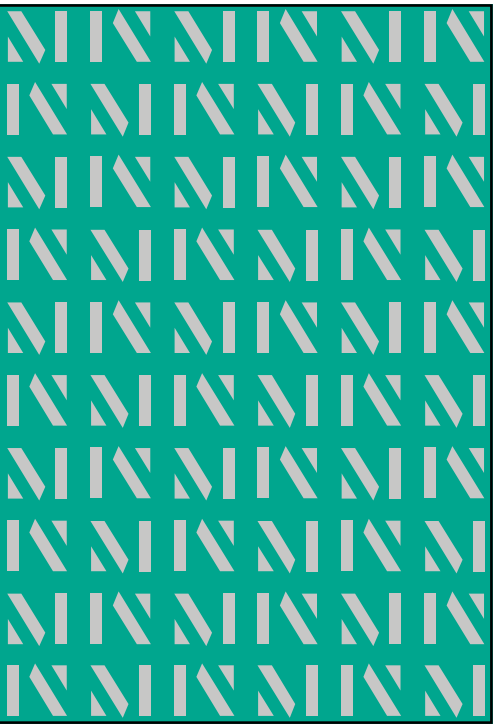
SOFTWARE QUALITY OVERSIGHT/INDEPENDENT REVIEW ORGANIZATION

- Assesses the company's ability to effectively test the implementation of its EHR software
- Assesses the company's compliance with its policies and procedures
- Maintains right of full and timely access to all persons, places, documents, records and information as deemed appropriate by Oversight/Review Organization, and to Covered Persons outside the company's/counsel's presence
- Completion/Submission of Baseline and Interval Assessment Reports

35

35

QUALITY AND COMPLIANCE RISKS AND MEASURES TO ADDRESS THEM



36

36

EXAMPLES OF QUALITY AND COMPLIANCE RISKS

- Prescription
- Inaccurate routing of test results
- Delayed testing and/or treatment
- Loss of clinical data from the record
- Patient record “scrambling”
- Improper billing

37

37

COMPLIANCE MEASURES FOR EHR DEVELOPERS

- Developing and implementing a compliance program that includes the systems, functions and activities that are identified in OIG’s current CIAs
- Prioritizing the development and implementation of functions and procedures for the prompt reporting of known and suspected patient safety, usability, and certification issues
- Issues must be timely identified and addressed, and fully remediated to prevent recurrence

38

38

COMPLIANCE MEASURES FOR USERS OF EHR SOFTWARE

- Developing organizational awareness that deficiencies, design flaws, usability problems and defects in the EHR software may impair the integrity and accuracy of the medical record and impact patient safety
- Implementing audit plans of EHR data/records
- Maintaining documentation and communicating with EHR developers regarding patient safety and other identified issues
- Performing periodic, independent auditing of EHR documentation to identify any integrity concerns and to ensure documentation complies with Federal health care program requirements

39

39

THANK YOU / QUESTIONS?

Felicia E. Heimer
Senior Counsel
Office of Counsel to the HHS
Inspector General
felicia.heimer@oig.hhs.gov

James A. Cannatti III
Partner, McDermott Will & Emery
202-756-8866
jcannatti@mwe.com

This material is for general information purposes only and should not be construed as legal advice or any other advice on any specific facts or circumstances. No one should act or refrain from acting based upon any information herein without seeking professional legal advice. McDermott Will & Emery® (McDermott) makes no warranties, representations, or claims of any kind concerning the content herein. McDermott and the contributing presenters or authors expressly disclaim all liability to any person in respect of the consequences of anything done or not done in reliance upon the use of contents included herein.
*For a complete list of McDermott entities visit mwe.com/legalnotices.

©2021 McDermott Will & Emery. All rights reserved. Any use of these materials including reproduction, modification, distribution or republication, without the prior written consent of McDermott is strictly prohibited. This may be considered attorney advertising. Prior results do not guarantee a similar outcome.

40