Part B Insider (Multispecialty) Coding Alert

Vendors: Create a Template to Rate Your EHR Vendor

Hint: EHR companies continue to be on the OIG's watchlist.

If you're considering switching to a new EHR vendor or changing cloud services provider, you may want to do some background research first. With cybersecurity issues dominating healthcare news over the last year, it is critical that practices keep a close watch on all their vendors to steer clear of fraud or security woes.

Why: Evidence and case settlements suggest that compliance relating to EHR vendors is firmly in the HHS Office of Inspector General's (OIG's) sights for 2021.

OIG: For example, consider this recent fraud issue - which isn't the first of its kind that the feds have settled. Miami-based EHR designer CareCloud Health Inc. f/k/a CareCloud Corporation settled False Claims Act (FCA) and Anti-Kickback Statute (AKS) allegations with OIG in April to the tune of $3.8 million. The firm offered providers kickbacks for referring others to their EHR products; plus "the kickback payments rendered false the claims submitted by CareCloud for federal incentive payments" associated with Medicare's Meaningful Use program and the Merit-Based Incentive Payment System (MIPS), indicates a Department of Justice (DOJ) release.

"Product functionality, reliability, and safety should drive a medical software company's success, not illegal kickbacks paid to promote its products," warns **Juan Antonio Gonzalez**, acting U.S. attorney.

Understand How OCR Looks at Vendors, Too

On top of OIG's interest, the HHS Office for Civil Rights (OCR) has long advocated for stronger vendor vetting as many cloud and EHR providers deal with patients' electronic protected health information (ePHI). Remember, "if the vendor does need access to the protected health information of the covered entity in order to provide its service, the vendor would be a business associate of the covered entity," and many software and cloud vendors fall into that category, OCR guidance says.

"If a business associate qualifies as an 'agent' of the covered entity that is providing the protected health information, the covered entity could potentially be liable for HIPAA violations of the agent," explains attorney **Shannon Hartsfield**, an executive partner with Holland & Knight LLP in Tallahassee, Florida.

"Even if the business associate is an independent contractor, the reality is that, if the business associate has a breach or otherwise does something wrong with data, it's likely going to create serious problems for the entity disclosing the data," Hartsfield warns.

Rate Your Vendors With These Tips

As part of your compliance planning and HIPAA risk assessment, it is a great idea to create a list of all your vendors annually and check in with them. And, if you don't know a vendor that well, "it may be prudent to ask whether the vendor has conducted a risk analysis and risk mitigation plan and how often it's updated," too, Hartsfield advises.

As part of the follow-up, you should do a comprehensive investigation of your EHR products, partner relationships, and

contracts. During this review, you may want to see whether your current vendors have had any compliance or violation issues over the past year of service.

While performing your re-evaluation, consider utilizing a specialty-specific template with weighted questions; then, you can tally your results before renewing your contract. Here are some examples of important questions to add to your vendor scorecard, inspired by guidance from the HHS Office of the National Coordinator for Health Information Technology (ONC):

- Does your current EHR vendor offer all the necessary functions your practice needs?
- What is the pricing model of your current EHR software, and does it match industry standards?
- Does your vendor offer certified EHR technology (CEHRT) in your specialty that aligns easily with the scope of your work?
- Is the EHR provider geographically positioned to consider your state's compliance requirements as well as the federal mandates?
- Does your software provider offer user-friendly clinical tools and is your practice using them properly?
- Is EHR training included in the package or is that extra? Are all employees allowed access to the educational materials?
- Has your EHR vendor been privy to a HIPAA, FCA, or AKS violation over the past year?
- If you're unhappy with the service or contract, will you be penalized for switching to another EHR vendor?
- Do you have a business associate agreement (BAA) on file with your EHR vendor?

Caution: "If an entity disclosing data to a vendor becomes aware of a pattern of problems with the vendor with respect to how the vendor is using or disclosing protected health information, HIPAA requires the disclosing entity to take reasonable steps to address the violation, and terminate the contract if those steps do not work," Hartsfield reminds.