

New Guidance on EHR Contract Negotiation Should Facilitate Implementation

November 2, 2016 Neil Issar

PRACTICES Healthcare and Life Sciences, Healthcare Transactions and Regulatory

Twelve years ago, the Department of Health and Human Services (HHS) established the Office of the National Coordinator for Health Information Technology (ONC) and called for the nationwide implementation of electronic health records (EHRs), or, in essence, a paperless healthcare system, within a decade. Use and functionality of EHRs have increased rapidly since then, buoyed by the financial incentives offered for healthcare providers that demonstrate meaningful use of EHRs pursuant to the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH). But large-scale adoption and application of EHRs still present certain challenges. For example, acquiring a new EHR system or updating an old one may require conversion of existing medical records, changes in the way documentation is handled, and new training of employees. Such activities often result in increased workload and costs and potentially lost revenue caused by disruptions associated with system conversion and integration with existing infrastructure.

These challenges and consequences can be exacerbated if providers do not obtain favorable agreements with EHR vendors, especially with cloud-based EHR systems in which providers often pay vendors a subscription fee to use the system rather than purchasing and installing the software themselves.² To this end, the ONC recently released a new guidance document entitled *EHR Contracts Untangled: Selecting Wisely, Negotiating Terms, and Understanding the Fine Print* (the “Guide”). The Guide addresses issues healthcare providers must consider when navigating the EHR implementation process and negotiating key vendor contract provisions.

The first steps in providers’ selection of an EHR system involve identification and prioritization of their technical and operational requirements and comparison of possible EHR systems and types. The ONC’s Guide explains why these steps are important for providers’ comprehension and communication of their needs to potential EHR vendors, which, in turn, serve as a framework for negotiating reasonable contract terms.

The Guide stresses that providers should not rely on a vendor’s demonstration of its product or the claims and statements made in a vendor’s marketing materials. Instead, providers must ensure that the EHR contract’s express terms reflect their needs, since the contract alone defines and limits parties’ rights and obligations. For example, a good contract will spread the responsibility for preventing and mitigating different safety risks among both parties, while also expressly referencing the specific amount and type of training provided by the vendor for its provider customers. The ONC previously released a guide explaining key EHR contract terms in 2013, and *EHR Contracts Untangled* supplements the agency’s resources to translate legal and contract terms into easy-to-understand language for providers.

The ONC’s Guide also emphasizes that providers should negotiate certain express warranties to create legally enforceable rights with respect to core EHR system performance expectations. This is important to ensure a vendor support when a provider faces problems such as system unavailability at critical times, a slow or unresponsive system affecting the ability to provide medical services, or the unavailability of important data. In addition, providers should attempt to obtain

guaranties that the vendor's system allows sharing and seamless integration of data from the provider's other sources—also known as interoperability—without the vendor being able to block the exchange of patient data or terminate system access.

The Guide covers different types of EHR systems, and explains the difference between on-site deployment (requiring providers to pay for ongoing costs to support and manage on-site data servers) and software-as-a-service (SaaS) deployment (typically requiring providers to pay a fixed monthly subscription cost). SaaS EHR solutions are growing in popularity, as they allow vendors to make upgrades and repairs without the provider's involvement while simultaneously allowing providers and staff members to access the system from remote locations.

But SaaS EHRs also mean the vendor stores all patient data and documentation. The Health Insurance Portability and Accountability Act (HIPAA) requires covered entities and business associates to enter into contracts with their business associates to ensure that protected health information is appropriately safeguarded (Business Associate Agreements).² The Guide, however, points out the value of negotiating terms related to data rights and information security as part of the EHR contract rather than relying solely on the provisions of Business Associate Agreements. This means contracts with vendors should include terms concerning the provider's exclusive ownership of data stored in, created by, or received by the EHR; control over the vendor's ability to de-identify and commercialize data; and the vendor's approach to data backup and disaster recovery. The contracts may also cover what would happen if a vendor is acquired by another entity, goes out of business, or otherwise encounters hurdles that affect its ability to deliver continuous service.³ More generally, EHR contracts should cover transition issues and how a provider can continue operation of its system and retain immediate access to all data in a variety of emergency scenarios.

Finally, the ONC's Guide explains how intellectual property (IP) provisions in an EHR contract not only protect providers but also outline the extent to which providers can customize or enhance their systems. The Guide emphasizes that EHR vendors should warrant that their software does not infringe on any patent, copyright, trademark, trade secret, or other IP right of any third parties. Vendors should also indemnify providers from all costs associated with infringement of such third party rights, as damages awarded in IP cases involving EHR software can reach millions of dollars.⁴ Relatedly, EHR contracts should include terms concerning limitations of liability and damages, management of risks, contract termination, and dispute resolution.

EHR Contracts Untangled provides valuable guidance for healthcare providers that are adopting an EHR system for the first time or upgrading and replacing existing technology. As EHR implementation and use continue to grow, the Guide will assist providers with better communicating their health information requirements to potential vendors, negotiating favorable contract terms, managing risks, and addressing security and intellectual property issues.

¹ See Sam Narisi, [Watch out for these common EHR contract pitfalls](#), HEALTHCARE BUSINESS & TECHNOLOGY (Aug. 13, 2013)

² A "business associate" is an entity or individual that performs certain functions or activities on behalf of a "covered entity" (e.g. health providers and insurers). 45 C.F.R. § 160.103.

³ Jenny Jackson et al., *Negotiating the EHR Vendor Contract*, 96 BULL. AM. COLL. SURG. 12, 14 (2011).

⁴ For example, a jury awarded medical software giant Epic Systems \$240 million in compensatory damages and \$700 million in punitive damages in a lawsuit against Indian IT provider Tata Consultancy Services for unauthorized access and use of confidential information and trade secrets. Epic alleged that Tata employees hired as consultants to help a Kaiser Permanente medical center implement an Epic EHR used their temporary access to Epic's databases to download confidential source code and data and then used this information to benefit Tata's competing EHR software. See *Epic Sys. Corp. v. Tata Consultancy Servs. Ltd.*, No. 14-cv-748-wmc, 2015 WL 7301245 (W.D. Wis. Nov. 18, 2015).