CLIENT ALERT

Don't Sign That Yet! – New HHS Guidance on Health IT Contracts

Sep.26.2016

The Office of the National Coordinator for Health IT (ONC) at HHS released guidance today – *EHR Contracts Untangled* – to help health care providers select and negotiate contract terms with technology vendors.

What Does This Mean for You?

This ONC contract guidance provides a new baseline for protecting against risks that can impact patient care or business efficiency, as well as preventing unanticipated operational challenges and unexpected costs. Many health care providers and EHR vendors entered into contracts quickly to comply with the Meaningful Use requirements. As a result, many of the issues raised in this guidance may not have been thoroughly considered in current agreements, and may lead to the misaligned expectations of both parties.

What's in the New Guidance?

The guidance aims to preempt some of the common missteps in the contracting process. It discusses key issues for consideration, includes suggested contract language, and even provides views on overall best practices. The guidance also raises the importance of considering other regulatory issues, such as HIPAA, Stark and the Anti-kickback Statute, health IT standards and certification rules, and Medicare payment rules, including MACRA and Meaningful Use. The guidance stresses that providers are strongly advised to consult legal, technical, and privacy advisors throughout the contracting process for details about compliance obligations that may need to be addressed. Here are some of the highlights:

1. Safety and Security – The responsibilities for safety and security should be shared between the parties. Consider assigning mitigation of risk to the party who has the most control over factors that may lead to a patient safety or security risk. Enable the reporting of safety or security risks to industry stakeholders, both as required by law and as reasonably necessary to improve operation.

2. System Performance – Ensure all core service and performance obligations are expressly and specifically stated in your contract, including system availability, response time, data integrity, and timeliness of implementation and maintenance.

3. Data Rights – Safeguard your ability to control and access patient data. Limit the EHR vendor's access and use rights to the minimum data necessary to perform its services and ensure providers and vendors agree on de-identification. Ensure contract terms are compliant with HIPAA and other regulations. Maintain provider and patient access to data, even when there is a dispute between the parties.

4. Interoperability and Integration – Make sure that the contract does not restrict the ability of the system to exchange data with current internal and external IT systems. Confirm that the system supports integration of data from third party sources outside of your network, such as through health information exchange organizations, remote monitoring tools, claims databases, clinical registries, and population health management tools.

5. Intellectual Property (IP) – Providers should secure the appropriate licenses for use of the EHR software to support their digital health strategy and to meet regulatory compliance obligations, such as the HIPAA patient access requirements and the Meaningful Use requirements. Ensure that the provider and vendor are aligned on ownership of any software customizations or other IP issues.

6. Liability – Conduct a risk assessment and fairly allocate risks and liabilities (including for HIPAA claims, patient claims, third party claims, and IP infringement) between the parties by appropriately structuring any "risk transfer" through indemnity provisions or otherwise. Consider the impact of this risk allocation on your insurance coverage.

7. Dispute Resolution – Clearly identify dispute resolution provisions to help ensure that problems are satisfactorily resolved in a manner that is beneficial, including being timely and cost-effective. Consider informal dispute resolution processes, such as mediation, and specify details for arbitration or litigation. Ensure the continuity of patient care and record access, as well as your business operations, during a dispute.

8. Transition Issues and Data Access – Include specific rights and obligations for an orderly transition to a different EHR vendor, including sufficient software licensing periods, the level of transition support services from the outgoing vendor, and data transfer to the new vendor's system.

This guidance has broader applicability to a variety of digital health tools. Crowell & Moring attorneys understand the health care and digital health market, and can help you assess your needs and renegotiate contracts or consider new acquisitions of digital health products and services. We can bridge the legal issues and your business needs, while helping you consider best practices and meet regulatory obligations.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jodi G. Daniel
Partner – Washington, D.C.
Phone: +1 202.624.2908
Email: jdaniel@crowell.com

Bryan Brewer
Partner – Washington, D.C.
Phone: +1 202.624.2605
Email: bbrewer@crowell.com