



The Office of the National Coordinator for
Health Information Technology

EHR Contracts Untangled

Selecting Wisely, Negotiating Terms, and Understanding the Fine Print

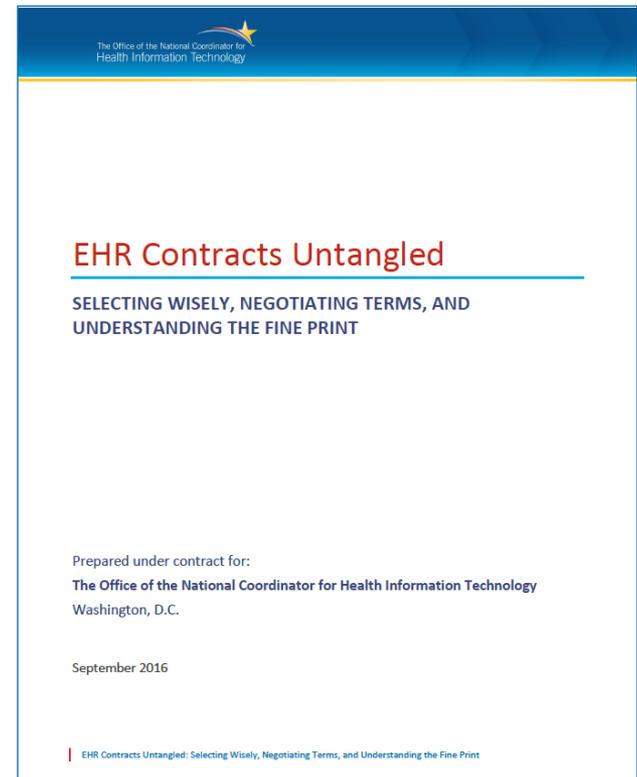
Elise Sweeney Anthony, Director of Policy, ONC
Karson Mahler, Senior Policy Advisor, ONC

October 2016



EHR Contracts Untangled: Selecting Wisely, Negotiating Terms, and Understanding the Fine Print

- Updates a guide released by ONC in 2013
- Prepared for ONC by private sector attorneys who have extensive experience negotiating EHR contracts
- A resource for diverse audiences



The EHR Contract Guide should not be construed as legal advice and does not address all possible legal and other issues that may arise with the acquisition of an electronic health record or other health information technology product or service. Each health care provider organization is unique and will need to consider its particular circumstances and requirements, which cannot be contemplated or addressed in this guide. A health care provider organization should obtain the advice of an experienced attorney whenever it proposes to enter into a legally binding contract.

EHR Contract Guide

Helps Health IT Purchasers:

- Understand the “fine print”
- Consider contract provisions that impact whether the technology they are contracting for will meet their needs and expectations
- Ask the right questions when selecting an EHR and better communicate their requirements to potential vendors
- Consider and manage expectations and offer a framework for negotiating reasonable contract terms that reflect best practice contracting principles

The guide is divided into two parts.

Part A: The Importance of Planning: Putting Your Best Foot Forward

- Highlights the critical planning steps that providers should take to properly understand and communicate their requirements to potential vendors.
Areas addressed include:
 - » Types of EHR products and service models
 - » Researching and comparing EHR products and vendors
 - » Identifying and prioritizing technical and operational requirements
 - » Understanding certification and regulatory requirements
 - » Procurement strategy, planning and resourcing

Part B: Negotiating EHR Contracts: Key Terms and Considerations for Providers

- Focuses on the negotiation and contracting phase of acquiring an EHR
- Contains strategies and recommendations for negotiating best practice EHR contract terms
- Addresses the practical issues important to providers
- Illustrates how legal issues might be addressed in a contract by providing example contract language

refund for any prepaid services. Example language to address these points is set forth below.

Example Contract Term 11

Neither party will be liable for any failure or delay in its performance under this Agreement due to causes beyond its reasonable control, including but not limited to, labor disputes, strikes, lockouts, shortages of or inability to obtain materials, energy, raw materials or supplies, fire, flood, war, terrorism, riot, act of God, or governmental action (such as a "Force Majeure Event"). provided, however, that (i) the Vendor may not rely on this provision if it has not maintained an implemented the disaster recovery plan and procedures as required by the Agreement. Customer shall not be obligated to pay any fees or other amounts for periods during which the EHR Vendor's performance is adversely affected by such a Force Majeure Event in any material respect. Customer may also, in its sole discretion, elect to terminate this Agreement and not be obligated to pay any amount referenced in hereunder for future services if a Force Majeure Event affects the EHR Vendor's performance hereunder in any material respect for more than _____ days. The Vendor shall also refund any amounts advanced and in advance for services that were not provided due to the Force Majeure Event and for any services that should be performed in the future if this Agreement is terminated due to a Force Majeure Event.

Another important protection is an "opt-out" warranty or service level agreement by which the vendor of a cloud-based EHR promises to make the EHR services available at a specific level (for example, 99.9% of the time). This protection is discussed in Section 2 - System Performance: Ensuring Your EHR Meets Your Expectations.

4.3 Avoiding Data Access Being Blocked

Some standard form EHR contracts grant the vendor the right to make the data unavailable or even terminate its services in the event of non-payment or other dispute (sometimes referred to as a "kill switch").¹⁰ Other standard form EHR contracts are silent on this issue, which creates a risk that a vendor can block data access or terminate the services when disputes arise. The type of conduct by an EHR vendor already could have a devastating impact on patient care and safety. Even the threat of terminating services or making data unavailable may give the vendor tremendous leverage in a contract dispute, especially in a cloud-based EHR.

To reduce the risk of data access being blocked by a vendor, you may wish to include language such as the following example in your EHR contract. If the vendor does not agree to this approach and you have a significant concern, then this may be a reason to consider another EHR vendor.

Example Contract Term 12

The Software and Services (and any portion thereof) do not and shall not in the future contain any virus, block, ransom, keylog, or spyware, including design, coding, device, or other mechanism that causes or could cause the Software, data, or Services for any portion thereof to become erased, corrupted, misused, or otherwise incapable of being copied or used in the full manner for which it was designed or required to be provided hereunder. "Disabling Technology" is the term of a breach of this provision, the EHR Vendor shall not use or permit any of the Disabling Technology to be used and shall, if the EHR Vendor's sole expertise, promptly remove the Disabling Technology and take all other action necessary to comply with this provision.

You may also wish to propose language requiring both parties to continue to perform their obligations in the event of a dispute as discussed in Section 2 - Dispute Resolution: Resolving Disagreements with Your EHR Vendor.

¹⁰ See, e.g., [HHS to Congress on Health Information Blocking Report](#), available at <https://www.hhs.gov/health-it/2018/03/01/hhs-report-2018-03-01>, [Blocking Health Data](#) (a person, service, or system is a "disabling blocking technology" is an example of information under which the operation of a "kill switch" was directed to curtail information blocking).

EHR Contracts: Unplanned, Unclear, Unlikely, Unsettling Terms, and Understanding the Fine Print 25

Areas covered in Part B of the guide:

- **EHR Safety and Security: A Shared Responsibility (B.2)**
 - » An EHR contract should assign appropriate roles and responsibilities to both the provider and the vendor, and should ensure that providers are not unreasonably prevented from reporting and discussing patient safety, security, and other issues.

Safety

- Ongoing maintenance, upgrades, performance monitoring and optimization.
- Internal controls and processes for software and upgrades.
- Investigation and collaboration in response to EHR technology-related deaths, serious injuries, or unsafe conditions.
- Transparency about problems.
- Training and education of users.

Security

- Security assessment questionnaire.
- Independent security audit.
- Provider's information security program and industry standards (e.g., NIST Common Framework) are baseline.
- Encryption methodology and secure data destruction.
- Compliance with all applicable state and federal data security regulations.

Areas covered in Part B of the guide:

- **System Performance: Ensuring Your EHR Meets Your Expectations (B.3)**
 - » The contract should reflect the promises that the vendor makes, including during negotiations, by expressly describing all core service and performance obligations.
 - Acceptance criteria
 - Uptime and system response time
 - Quality and timeliness of service
 - Post implementation support
 - » Providers can explore performance management strategies – e.g., SLAs for unscheduled system downtime

Areas covered in Part B of the guide:

- **Data Rights: Managing and Safeguarding EHR Data (B.4)**
 - » The contract should reflect the principle that, as between the provider and vendor, the provider owns all EHR data and has timely and reliable access to it.
 - » An EHR contract should not impede a provider from extracting maximum analytical value out of its data, and from fulfilling its role as custodian of its patients' health information.
 - Acknowledge the importance of data in patient care
 - Control the scope of commercialization by vendor
 - Respond to emergencies
 - Facilitate patient access
 - Prevent data access being blocked

Areas covered in Part B of the guide:

- **Fostering Interoperability and Integration (B.5)**
 - » An EHR contract should not unduly restrict a provider's ability to integrate third party technologies and services that are important to the provider's ability to leverage data to deliver better and more efficient care, or to take advantage of emerging technologies .
 - Interface strategy – point-to-point, data feed or batch export capabilities, APIs.
 - Integrating third party products.

Areas covered in Part B of the guide:

- Intellectual Property Issues (B.6)
 - » An EHR contract should recognize the investments that a health care provider makes in customizing or improving their EHR by granting the provider appropriate rights in those customizations and improvements.
 - Limited license v. perpetual license v. ownership. (CONSIDER THE SCOPE OF THE LICENSE FROM THE VENDOR)
 - » An EHR contract should provide the provider with sufficient rights to use all of the vendor's IP that is necessary to support the provider's obligations under HIPAA and impending Meaningful Use and other federal or state requirements.
 - » Contract terms that address the consequences of IP claims made by third parties should be carefully considered. (necessary to provide the software or service without "infringing" or violating the IP rights of others, you could be sued.)

Areas covered in Part B of the guide:

- **Managing Risks and Liability (B.7)**
 - » One party to an EHR contract should not bear all of the risk for the performance of the EHR—risk and liability should be allocated fairly between a provider and vendor so that risks are born by whichever party has most control over and ability to mitigate the risk.
 - Indemnities should reflect the principle of comparative negligence (each party is responsible for its own negligent acts or omissions).
 - Dollar amount limitations should be based upon the true maximum amount of financial risk exposure.
 - Carve outs for limitation of liability provisions are appropriate (e.g., personal injury, breach of HIPAA, willful misconduct).

Areas covered in Part B of the guide:

- **Dispute Resolution: Resolving Disagreements With Your EHR Vendor (B.8)**
 - » Well drafted dispute resolution provisions can help ensure continuity of patient care and the provider's business operations.
 - Continuity of service
 - Litigation v. arbitration

Areas covered in Part B of the guide:

- **Transition Issues: Switching EHRs (B.9)**
 - » An EHR contract should facilitate the transition—with minimum cost and disruption—if a provider chooses to switch EHRs (e.g., at the end of their contract).
 - Getting the contract structure right – length of support commitment
 - Transition assistance – data transfer and conversion
 - Accessing previous versions of EHR software