The Office of the National Coordinator for Health Information Technology

EHR Contracts Untangled

SELECTING WISELY, NEGOTIATING TERMS, AND UNDERSTANDING THE FINE PRINT

Prepared under contract for:

The Office of the National Coordinator for Health Information Technology

Washington, D.C.

September 2016

Disclaimer

This guide was developed under contract for the Office of the National Coordinator for Health Information Technology. It 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.

TABLE OF CONTENTS

INTRODUCTION

Selecting and negotiating the acquisition of an electronic health record system (EHR) is a challenging but important undertaking for any health care provider organization. At their best, EHRs and other health information technologies (health IT) can make information actionable and available when and where it is needed to transform the way care is delivered. However, these technologies may not always meet expectations. The experiences of some health care provider organizations can serve as a cautionary tale of the challenges faced when selecting, acquiring, implementing, and using a new EHR:

- a regional health system made the news when its difficulties implementing a new EHR led to the resignation of the system's CIO and CEO. A lack of clinician consultation, an aggressive implementation timeframe, and user training problems reportedly contributed to serious communications and recordkeeping issues, including medication errors, orders being lost or overlooked, and patients leaving the emergency department after long waits.
- a small rural primary care provider was taken by surprise when it discovered that it had been locked out of its cloud-based EHR. A dispute over the provider's refusal to pay maintenance fees resulted in the EHR vendor deploying disabling technology that prevented the provider from looking up the medical histories of its 4,000 patients.
- a cloud-based EHR was affected by a two day Internet brown-out that resulted in certain customers having only intermittent access to their EHR, with some practitioners cancelling an entire day's worth of patient visits.

This guide will help you understand how to manage these types of risks via your EHR contract so that you can maximize the value of your health IT investment, whether you are acquiring your first EHR or upgrading or replacing your existing technology. It offers strategies and recommendations for negotiating best practice EHR contract terms and illustrates how legal issues might be addressed in a contract by providing example contract language.

What type of technology does this guide address? This guide focusses on the acquisition of an electronic health record system—referred to in this guide as an "EHR." Many of the concepts and example contract terms in this guide may also apply to other types of health IT products and services. In this guide, the term **EHR** refers to a system that supports a health care provider organization's management and use of patients' longitudinal health records and other electronic health information. An EHR typically comprises an integrated data repository and the software applications through which the data, together with other information and clinical and management tools, are accessed and maintained. EHRs may be purchased or licensed from a single vendor or from multiple vendors and come in a variety of architectures and service models—some common examples of which are discussed below in Part A. As you contemplate the acquisition of an EHR, it is critically important to recognize that the EHR will need to operate within the context of a larger health IT system. This will require the EHR to be interoperable with other IT systems and/or software applications as well as to integrate data from other clinical information systems or databases.

Who is this for? Health care professionals and other decision-makers, as well as their advisors, who are responsible for planning and negotiating the acquisition of an EHR or other health IT services. When this document uses the term "you," it means a health care provider organization that acquires or uses the EHR or other health IT. It is assumed, for the purpose of this guide, that your health care provider organization or practice is a "covered entity" and subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Notwithstanding this, many of the issues discussed in this guide apply equally to health IT contracts to be entered into by provider organizations that are not subject to HIPAA.

Why should you read this? Investing in the preparation, planning, and negotiation of an EHR acquisition can minimize business and patient safety risks. This guide can help you better understand and communicate your EHR requirements to potential vendors, negotiate appropriate contract terms that protect your interests, and manage risks that may arise in the implementation and use of your EHR. It

does not cover the decisions that you may need to make to design (or redesign) your organization's workflows and related policies and procedures when implementing or using your EHR.

What else do you need to know? The purpose of this guide is to enhance your understanding of core issues when selecting an EHR, including key elements of EHR contracts that require careful consideration and negotiation in order to get optimal value from your EHR and EHR vendor. Example contract terms have been included in this guide to illustrate how you might address certain issues in your EHR contract. The example contract terms will need to be tailored to meet your specific circumstances and the EHR model you have selected.

This document is not a complete description of standard contract terms, nor does it address all matters to be considered when acquiring an EHR. For example, at the same time as you negotiate an EHR contract for the services to be delivered by your EHR vendor, you must also reach agreement with your EHR vendor about certain rights and obligations to appropriately safeguard protected health information (PHI) in accordance with the requirements of HIPAA. This agreement, referred to as a "Business Associate Agreement" (BAA), also serves to clarify and limit, as appropriate, the permissible uses and disclosures of PHI by your EHR vendor. Most health care provider organizations and EHR vendors prepare a separate contract reflecting the requirements of a BAA, but it is also valid to incorporate all or part of your BAA into your EHR contract. While this guide discusses certain privacy and security issues in the context of the service obligations to be fulfilled by your vendor, a full discussion of your and your EHR vendor's obligations under the HIPAA Privacy Rule and HIPAA Security Rule, and the requirements of a BAA, is beyond the scope of this guide. There are additional rights and obligations that must be addressed under your BAA that are not addressed in this guide. Further information on your HIPAA compliance obligations, including links to useful resources, is provided in Part A below.

This document should not be construed as legal advice[1] and does not address all possible legal and other issues that may arise with the acquisition of an EHR. Because every health care provider organization is unique with respect to its operations, priorities, resources, and IT infrastructure, your acquisition, implementation, and use of an EHR will present issues specific to your practice or organization that cannot be contemplated or addressed in this guide. **You are strongly encouraged to obtain the advice of an experienced attorney whenever you are proposing to enter into a legally binding agreement for health IT products or services.**

In addition to legal advice, you may benefit from technical advice regarding your organization's EHR requirements, which can help you understand the EHR marketplace and better inform you of the capabilities and limitations of products being offered by EHR vendors.

[1] The substantive parts of Part B of this document were written by Elisabeth Belmont, J.D., and Marilyn Lamar, J.D. Ms. Belmont has extensive experience in electronic health information network strategy development and implementation to support innovations in care delivery and payment models as well as information technology acquisitions and licensing. Ms. Belmont is a National Associate of the National Academies of Sciences, Engineering, and Medicine, a past President of the American Health Lawyers Association, and a past Chair of the Association's Health Information and Technology Practice Group. Ms. Lamar has negotiated on behalf of providers with EHR technology developers over many years. Ms. Lamar is President Elect-Designate of the American Health Lawyers Association and a past Chair of the Association's Health Information and Technology Practice Group. Ms. Belmont and Ms. Lamar were assisted by Robert Dearn, who also wrote the substantive parts to this Introduction and Part A. Mr. Dearn is an Australian qualified lawyer who has practiced extensively in health technology and health services contracting, as well as health privacy and technology licensing. Mr. Dearn has advised the Australian Government and consulted to the US Government on health IT regulation. This document reflects their collective experience, but it does not constitute legal advice.

PART A – THE IMPORTANCE OF PLANNING: PUTTING YOUR BEST FOOT FORWARD

The success of your EHR acquisition may be determined well before you sit down with your preferred EHR vendor to hammer out a contract. Before you embark on contract negotiations (which are covered in **Part B**) you should ensure that you:

- have researched the EHR market, including competing vendors, products, and services, together with price and service terms;
- have assessed your organization's need for and readiness to implement or to transition to a new EHR;
- have a vision and plan for how the EHR will support your needs, which should be informed by input from clinical, administrative, IT, and other relevant representation throughout your organization;
- have prepared a priority checklist of features and functionality you want in your EHR;
- understand the importance of health IT certification and the regulatory requirements impacting EHR acquisition and use; and
- understand the security and privacy requirements that apply under both federal and state laws and regulations, and the best practices that you desire above and beyond legal minimums.

(i) The EHR Market: Types of Products and Service Models

The delivery of an EHR is typically achieved under two broad service models:

Provider-hosted EHR. Under this model, often referred to as the "client-server model," EHR software is licensed to a health care provider organization, operated on the provider organization's own equipment, and accessed over a local area network. The health care provider organization hosts the EHR software, together with all data captured and records created in the EHR, on dedicated provider-owned or leased servers. Provider-hosted EHRs are sometimes contracted for under a software license together with a separate support or maintenance agreement.

Cloud-based EHR. The essential feature of this model is that the EHR—including the software and all data captured by and all records created in the EHR—is hosted on servers maintained by the EHR vendor and accessed by a health care provider organization via the Internet. Some cloud-based EHRs, often referred to as using the **"application service provider"** or **"ASP"** model, offer customers the opportunity to run a customer specific iteration of the EHR software and to host the EHR on dedicated servers. Other cloud-based EHRs, sometimes referred to as using the **"software-as-a-service"** or **"SaaS"** model, are provided "off-the-shelf," so that the EHR vendor may deliver an identical EHR platform to multiple customers simultaneously.

You may find variations on these models, or be offered a combination of elements from more than one EHR service model. You should carefully examine the potential benefits, limitations, and trade-offs of competing service models in light of your particular needs and circumstances.

The EHR service model you choose will impact the types of issues that you will need to address as part of your EHR contract negotiations, which are discussed in Part B of this guide. For example:

- Provider organizations using an off-the-shelf cloud-based EHR may have very limited opportunities to customize their EHR or to integrate their EHR and data with other third party technologies and services. In contrast, provider-hosted EHRs may offer significant customization opportunities, provided that appropriate intellectual property and data access rights are negotiated under the EHR contract (see *Section 5 – Fostering Interoperability and Integration* and *Section 6 – Intellectual Property Issues*).
- Because data is held and controlled by the EHR vendor under the cloud-based EHR model,

health care provider organizations are wholly reliant on their EHR vendor to make the EHR available where and when it is needed. This risk can be reduced by negotiating appropriate warranties, service-level agreements, and data access rights (see *Section 3 – System Performance: Ensuring Your EHR Meets Your Expectations* and *Section 4 – Data Rights: Managing and Safeguarding Your EHR Data*).

- There are security trade-offs between the two models that should be considered when selecting an EHR and negotiating appropriate contractual requirements. For example, a cloud-based system's economies of scale may have the potential to offer higher levels of physical, technical, and administrative security for data stored on the EHR vendor's servers than you may be able to provide for a local area network in your facility. On the other hand, cloud-based systems may be perceived as being at greater risk from cyber criminals because of the volume of data contained in them (see *Section 2 – EHR Safety and Security: A Shared Responsibility*).

(ii) Identifying and Prioritizing Your EHR's Technical and Operational Requirements

Selecting the right EHR requires you to analyze your organization's needs and understand how different EHRs meet them. This may require soliciting input and perspectives from staff throughout your organization and reflecting on how your organization's current IT environment, legacy systems, workflows, and organizational culture will impact the deployment of any new EHR. If applicable, it is important to consult with specialists such as pediatric or behavioral health professionals to understand any specialty-specific needs that your EHR will need to fulfil. The Department of Health and Human Services' (HHS) Office of the National Coordinator for Health Information Technology's (ONC) Health IT Playbook website (https://www.healthit.gov/playbook) provides a range of resources to assist health care provider organizations to identify and prioritize their EHR requirements.

It is also important to consider the role your EHR will play in enabling your organization to participate in new payment and care delivery models. In particular, you may need to integrate your EHR with other health IT services, now or in the future, to integrate health information from other sources and to use the data in your EHR to improve quality, increase efficiency, identify and close gaps in patient care, and participate in activities to improve public health. You should identify and communicate these requirements to potential EHR vendors—for example, via a statement of requirements in your request for proposal (RFP) documentation—to set clear expectations regarding the EHR vendor's role in facilitating interoperability and integration with other vendors, technologies, and services. These issues are discussed in detail in *Section 5 – Fostering Interoperability and Integration*.

Once you have identified the technical and operational requirements to be met by your EHR, and matched those requirements up with a vendor's EHR offering, it is critical that all of your requirements are reflected in your negotiated contract. Most EHR contracts are drafted on the basis that the parties' rights and obligations are limited to those expressly described in the EHR contract. **This means that you cannot rely on the claims and statements made in your vendor's marketing materials, nor on the functionality or performance you witnessed in your EHR demonstration, unless they are expressly promised (warranted) in your EHR contract**.

Accordingly, before starting your contract negotiations, it is useful to document in a complete and detailed manner the service components, technical specifications, and functional requirements that you understand you will be receiving as part of your EHR so they can be recorded in the contract itself. A common method of doing this, but not the only method, is to require that the relevant specifications, descriptions, or marketing materials be attached to your EHR contract as an exhibit and incorporated therein by reference.

(iii) Due Diligence: Finding the Best EHR for Your Needs

EHR customers have historically lacked accurate and readily-available up-front information with which to compare the costs, limitations, and trade-offs of competing EHRs. Transparency requirements under the ONC Health IT Certification Program require EHR

vendors to publicly disclose certain information about the limitations and types of costs of their health IT. This information can help you to compare EHRs and to conduct due diligence to avoid hidden costs or limitations. Health IT product disclosure statements must be published by EHR vendors on their websites and can also be accessed via ONC's transparency website (https://www.healthIT.gov/transparency).

In addition to publishing mandatory disclosure statements, some EHR vendors have committed to supporting additional, voluntary actions to increase transparency and provide potential customers with better comparative information about health IT products and services. For example, many vendors have taken a transparency attestation, signaling their commitment to open dialogue about costs, technical capabilities, and business practices, and to making such information available in more targeted and useful ways. You can take advantage of these commitments by asking EHR vendors to provide you with information about their products and services that is tailored to your specific circumstances and needs. A list of the vendors who have supported the transparency attestation is available on ONC's transparency website (https://www.healthIT.gov/transparency).

(iv) The Importance of Using a Certified EHR

Choosing EHR technology that has received certification under the ONC Health IT Certification Program provides you with assurances that your preferred EHR meets the technological capability, functionality, and security standards adopted by the Secretary of the Department of Health and Human Services. You can find certified health IT products on ONC's Certified Health IT Product List (CHPL) website (https://chpl.healthit.gov).

ONC's authorized certification bodies (ONC-ACBs) conduct ongoing "in-the-field" surveillance of all certified health IT products to ensure that products continue to meet certification requirements when used in live operational environments. You can investigate how an EHR has performed against its certification criteria "in the field" by visiting the CHPL website (https://chpl.healthit.gov).

Eligibility for participation in certain Federal health care incentive programs requires use of certified EHR technology. For example:

- Under Stage 3 of the Medicare and Medicaid EHR Incentive Programs (commonly referred to as the "Meaningful Use" program), patients must be able to access their health information using a computer application of their choice. To support this requirement, the ONC 2015 Edition final rule [2] adopted new interoperability certification criteria that provided that EHRs certified to the 2015 Edition are required to facilitate "application access" to certain health information (the Common Clinical Data Set) via an application programming interface (API).
- A new framework for compensating health care professionals for value-based care was established with the enactment of the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA). Under proposed rules published by the Center for Medicare and Medicaid Services (CMS) [3], health care professionals participating in the MACRA Merit-based Incentive Payment System (MIPS) or Alternative Payment Models (APMs) will receive payment based on quality and value. Congress called for the use of certified EHR technology in MIPS and in APMs under the MACRA.

You should be aware that, under the ONC Health IT Certification Program rules, a certification issued for a health IT product is not perpetual, and that an EHR vendor needs to meet ongoing requirements to maintain its EHR's certification. The failure of your vendor to maintain certification and comply with other federal requirements could preclude you from meeting eligibility requirements or submitting claims for reimbursement under federal health care programs that require the use of certified EHR technology. Because these programs may be updated

[2] 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications, Final Rule, 80 Fed. Reg. 62601 (Oct 16, 2015).

[3] Medicare Program; Merit-Based Incentive Payment System (MIPS) and Alternative Payment Model (APM) Incentive Under the Physician Fee Schedule, and Criteria for Physician-Focused Payment Models, Proposed Rule, 81 Fed. Reg. 28161 (May 09, 2016).

over time, placing different demands on you and your EHR, you should satisfy yourself that your preferred EHR vendor is contractually committed to updating your EHR to meet applicable requirements and that you understand any additional costs you may incur for such updates.

(v) Accepting Subsidies for EHR Products and Services

It is not uncommon for large health care provider organizations to offer to subsidize (or "donate") a portion of a smaller health care provider organization's costs of acquiring the organization's EHR, health IT, or related training services. Such an arrangement may be attractive for many reasons, but you should be aware that accepting a subsidized EHR will usually limit your choice of EHR vendor and, just as important, your ability to negotiate specific EHR contract terms. For the reasons discussed in **Part B**, this could have significant ramifications for you and your organization. For example, you may be unable to negotiate terms that are important to you, such as terms related to information exchange or shared responsibility for patient safety and the security of electronic health information. You may also experience challenges if your EHR arrangement does not facilitate a seamless transition to a new EHR should you decide to switch, including managing the separating out of patient charts and other records. It is important that you understand and consider these implications when deciding whether to accept a subsidized EHR.

If you do decide to accept a subsidized EHR, you need to exercise extreme caution to ensure compliance with applicable state and federal law. You should ensure, among other precautions, that the subsidy arrangement complies with the Federal Anti-Kickback Statute (AKS),[4] the physician self-referral statute[5] (commonly known as the "Stark Law"), as well as any applicable state law counterparts. These laws permit certain health care provider organizations to receive subsidized health IT items and services, but only when very specific conditions are met. For more information, see the resources available on the HHS Office of Inspector General's fraud and abuse website (https://oig.hhs.gov/compliance/physician-education/01laws.asp) and CMS' Stark law website (https://www.cms.gov/Medicare/Fraud-and-Abuse/PhysicianSelfReferral/index.html?redirect=/physicianselfreferral/).

(vi) Keeping Patient Information Safe and Secure: Complying with HIPAA

Many of the benefits of EHRs can be realized only if providers and patients have trust that individuals' electronic protected health information (PHI) will be private and secure. Central to achieving this level of trust is a health care provider organization's compliance with the Privacy, Security, and Breach Notification Rules promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), collectively known as the "HIPAA Rules." The HIPAA Rules provide federal protections for the PHI held by most health care provider organizations[6] (and their business associates) and also give patients an array of rights with respect to their PHI, including rights to access, obtain copies, and request corrections.

Information about the HIPAA Rules can be found at the HHS Office for Civil Rights'[7] health information privacy website (http://www.hhs.gov/hipaa). Additionally, ONC has a dedicated Health IT Privacy and Security Resources webpage (https://www.healthit.gov/providers-professionals/ehr-privacy-security/resources), which provides references to detailed educational materials and practical tips to help your organization with privacy and security. On that webpage you will find the ONC Privacy & Security Guide, published with the assistance of the HHS Office for Civil Rights. Chapter 6 of the ONC Privacy & Security Guide discusses security in detail, including questions to ask your EHR vendor.

[4] 42 U.S.C. § 1320a-7b(b).

[5] 42 U.S.C. § 1395nn.

[6] Healthcare providers are required to comply with the HIPAA Rules so long as they meet the definition of a "covered entity" for the purposes of HIPAA. Covered entities are healthcare providers who conduct certain standard administrative and financial transactions in electronic form, including doctors, clinics, hospitals, nursing homes, and pharmacies. Any healthcare provider who bills electronically (such as a current Medicare provider) is a covered entity. 45 C.F.R. § 160.103.

[7] The HHS Office for Civil Rights is responsible for administration and enforcement of the HIPAA Rules.

If you are a covered entity and your EHR vendor will have access to, use, or disclose PHI on your behalf, your EHR vendor will be a "business associate"[8] for the purposes of HIPAA.[9] Before you disclose any PHI to your EHR vendor you will need to enter into a written contract with it called a Business Associate Agreement (BAA) to safeguard PHI in accordance with the requirements of HIPAA. You can find details about the obligations of a business associate at the HHS Office for Civil Rights' health information privacy website (http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html) and in the ONC Privacy & Security Guide, which is also accessible through the Health IT Playbook website (https://www.healthit.gov/playbook). Model BAAs are available at http://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html. You should ensure that the terms of your BAA are incorporated into your EHR contract, for example as an exhibit incorporated by reference, and that it is expressly stated in your EHR contract that the BAA takes precedence in the event of any conflict or inconsistency.

(vii) Procurement Strategy, Planning and Resourcing

You should establish and implement a sound procurement strategy for your EHR acquisition. Your ability to influence the outcome of your EHR contract negotiations will largely depend on your knowledge of key concepts and on your negotiating leverage relative to the vendor, as well as on the resources you have allocated to the process. However, by using a sound and strategically framed procurement process, you can increase your leverage in any negotiation and improve your prospects of maximizing optimal value from your EHR acquisition. For example, often a very simple but effective technique in your procurement strategy is to identify a "Plan B"—whether it be continuing to receive services from your existing EHR vendor for an additional period or progressing negotiations with an alternative vendor—should your preferred vendor refuse to negotiate on aspects of the EHR contract that you feel would otherwise expose your organization to inappropriate risk or exposure. Having the ability to walk away from negotiations immediately increases your leverage and gives your organization's decision makers options to consider when reaching a final decision. You can visit ONC's Health IT Playbook website (https://www.healthit.gov/playbook) to access a range of resources to assist health care provider organizations to appropriately plan and resource the acquisition of an EHR.

[8] A business associate is directly liable under certain HIPAA Rules and subject to civil and, in some cases, criminal penalties for making unauthorized uses and disclosures of PHI or failing to safeguard electronic PHI.

[9] The only exception is where your EHR vendor simply provides you with software and plays no role in the installation, testing or maintenance of the software and will at no time be given access to PHI held by you. Because this scenario is extremely rare, it has been assumed for the purpose of this guide that you are a covered entity and that your EHR vendor will be a business associate for the purposes of HIPAA.

PART B – NEGOTIATING EHR CONTRACTS: KEY TERMS AND CONSIDERATIONS FOR PROVIDERS

1. INTRODUCTION TO EHR CONTRACTING

An EHR contract outlines the respective rights and responsibilities of a health care provider organization and its EHR vendor, and creates a binding obligation on both parties with respect to the acquisition, implementation, and use of an EHR, as well as related transition issues.

A carefully negotiated EHR contract can minimize the potential for future problems and create a more beneficial and balanced relationship between the EHR vendor and the health care provider organization. Increasingly, customers are expecting EHR vendors to fairly allocate risks and associated liabilities between the parties to reflect the shared responsibilities of an EHR implementation. As a customer, you should expect your EHR vendor either to offer, or be willing to negotiate, terms that are consistent with the best practices identified in this guide. To the extent that you negotiate a well-drafted, comprehensive contract with the EHR vendor, then it will serve as a roadmap for the parties' dealings during the implementation of the EHR as well as during its ongoing maintenance and use.

1.1 Standard Form EHR Contracts

Some EHR vendors use "standard form" contracts, where the terms and conditions of the proposed EHR contract are prepared by the vendor, and the provider organization has limited ability to negotiate more favorable terms and is thus placed in a "take it or leave it" position. Your ability to negotiate changes to an EHR vendor's standard form contract may depend, in part, on the following factors: (i) the importance of your business to the EHR vendor; (ii) the size of your practice or provider organization; (iii) the amount being spent on the acquisition; and (iv) the market share of the EHR vendor.

It is preferable to ask an EHR vendor for information regarding its contracting practices early in your EHR acquisition process and before you have identified your preferred EHR vendor. It is a matter for you to decide whether or not you choose to work with an EHR vendor that offers only a non-negotiable contract. If you decide to accept standard form EHR contract terms without modification, you should make sure you understand the nature of the rights and obligations to which you are agreeing. Additionally, it is important that you consider what might be missing from the standard form contract (using this guide as a starting point) and assess the risk to your organization caused by an EHR contract drafted from the vendor's perspective.

1.2 Negotiation Strategy

All EHR contract negotiations will require each party to make certain decisions based upon its particular needs and goals; terms that are perceived as critical by one health care provider organization may be less important to another. Prior to commencing negotiations for an EHR, you should understand and prioritize terms that are important to achieving your particular needs and goals with respect to the acquisition and implementation of an EHR.

You should also assess your negotiating leverage and the extent to which you are prepared to compromise in some areas to achieve a more favorable outcome in others. If you work with an EHR vendor that will negotiate contract terms, your negotiating leverage is likely to vary depending upon a number of factors—your circumstances and available resources, the EHR vendor's standard contract terms, how much you know about alternative contract terms, your skill at negotiating, and state law, among other considerations. Prior to negotiating the terms of the EHR contract, you and your acquisition team should prepare an issues list or negotiation matrix that documents your initial and fallback positions on each key issue arising in the contract. To increase your negotiating leverage, you may wish to consider not naming a specific EHR vendor as the "vendor of choice" and conducting parallel negotiations with more than one EHR vendor consistent with your available resources and timeline. You also may wish to have a discussion with senior management regarding your organization's willingness to walk away from an EHR contract negotiation if the vendor

is not responsive to your concerns or is unwilling to accept revised terms that are important to you. Consulting with an experienced attorney for legal advice is recommended.

1.3 Example Contract Terms

Example contract terms have been included in this guide to illustrate how you might address certain issues in your EHR contract. The example contract terms will need to be tailored to meet your specific circumstances and the EHR model you have selected. For example, the example contract terms employ capitalized words and phrases, some of which are not defined in this guide. If you negotiate contract terms modeled on the examples in this guide, you will need to carefully review how these capitalized words and phrases are defined in your EHR contract to ensure that they are consistent with the intent of those terms. Some of the example contract terms included in this guide address privacy and security issues that overlap with the issues addressed in a typical Business Associate Agreement (BAA). However, you should be aware that there are additional privacy and security rights and obligations that must be addressed under your BAA that are not addressed in the example contract terms. It is recommended that you seek legal advice on whether an example contract term is appropriate for your specific circumstances.

1.4 Technical Advice

In addition to legal advice, you may benefit from consulting with a technical advisor regarding your EHR acquisition to: (i) minimize problems during the initial and post "go-live" periods; (ii) anticipate your future needs with respect to your EHR, including customizations and other technology provided by independent vendors that may complement the core system; and (iii) design options to ensure that patient information can be transitioned if the technology becomes outdated or if it becomes necessary to change EHR vendors.

This document 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 EHR; each health care provider organization is unique with respect to its information technology infrastructure and the EHR license and implementation presents its own particular circumstances. This guide contains examples of certain contract terms favorable to health care provider organizations as well as a description of certain issues to consider in drafting key contract provisions. The examples and issues for consideration will need to be tailored to meet your specific circumstances.

2. EHR SAFETY AND SECURITY: A SHARED RESPONSIBILITY

Health IT is a powerful tool for improving the safety and efficacy of patient care; but similar to other innovations, it can also introduce new risks and potential sources of harm. Your EHR contract can help you mitigate these risks by, among other things, assigning appropriate roles and responsibilities to ensure the safety and security of your EHR and other health IT.

2.1 Shared Responsibility for Safety and Security

Assigning complete responsibility for performance to either the EHR vendor's technology or to the health care provider organization's implementation or use of the technology is inappropriate, because overall performance is based on their combined actions. By their nature, EHRs are deployed with other third party hardware and software and interact in complex ways with people and workflow processes within the local environment in which they are implemented. EHRs also operate in an environment of rapidly increasing security and cybersecurity threats. As a result, many factors affect the safe and secure use of EHRs, including: (i) the design, development, and configuration of hardware and software components; (ii) the manner in which these components are implemented and used; and (iii) the extent to which effective processes are in place to monitor and improve the use of the EHR and associated outcomes.

Indeed, a 2011 report by the Institute of Medicine (IOM Report)[10] concluded that ensuring health IT is

[10] Institute of Medicine, Health IT and Patient Safety: Building Safer Systems for Better Care (National Academy Press, 2012).

used safely to improve patient care is a shared responsibility among many stakeholders, including health care provider organizations, EHR vendors, health IT developers, and health care and IT professionals, among others. Similarly, Congress, in the Cybersecurity Information Sharing Act of 2015 (CISA),[11] recognized that the health care sector, which includes you, other providers, and EHR vendors, could benefit from more widespread and comprehensive sharing of identified cyber security threats.[12]

2.2 Ensuring Safe Implementation and Use

From a contractual perspective, the party who has the most control over the factors giving rise to a health IT patient safety risk is in the best position to prevent and mitigate such a risk. It is this party that an EHR contract should charge with responsibility for preventing or mitigating safety risks. When selecting a preferred EHR vendor, you should consider the willingness of a particular EHR vendor to agree to incorporate language in your EHR contract to address the following issues to minimize the associated risks and promote the safe use of EHRs:

- defining and documenting the roles played by the EHR vendor and by your health care provider organization and administrative and clinical personnel in ensuring the safe deployment, implementation, and use of the EHR, including ongoing maintenance, upgrades, performance monitoring and optimization;
- requiring that the EHR vendor maintain appropriate internal controls and processes to ensure the quality and safety of the EHR software and upgrades;
- requiring that the EHR vendor cooperate with and assist you in the investigation of EHR technology-related deaths, serious injuries, or unsafe conditions, including reasonable cooperation, where applicable, with obligations to report health safety issues to government agencies;
- requiring that the EHR vendor timely notify you and take other appropriate actions whenever the vendor identifies or becomes aware of software deficiencies, hardware defects, implementation errors, poor design or usability, misinterpreted user-technology interfaces, or other causes that could potentially affect patient safety;
- allocating responsibility within the EHR vendor's own organization for collaborating with your health care provider organization and personnel to provide timely solutions for identified patient safety issues (e.g., workflow guidance, features that should not be used, software updates) and to ensure that these solutions are provided to all users of the EHR; and
- allocating responsibility for ensuring adequate training and education of users, and appropriate resourcing, customization, and use of the EHR in accordance with risk assessment, developer recommendations, and your organization's EHR-related policy.

An example of a contract term focusing on the safe implementation and use of an EHR follows:

Example Contract Term 1

During the term of this Agreement, the EHR Vendor shall be responsible for the following: (i) maintaining appropriate internal controls and processes to ensure the quality and safety of the EHR Software and upgrades; (ii) notifying Customer in a timely manner whenever the EHR Vendor identifies or becomes aware of software deficiencies, hardware defects, implementation errors, design or usability issues, misinterpreted user-technology interfaces, or other causes that may negatively affect patient care; (iii) collaborating with Customer to provide timely solutions to identified patient safety issues (e.g., workflow guidance, features that should not be used, software updates); and (iv) cooperating with and assisting Customer in the investigation of EHR technology-related deaths, serious injuries, or unsafe conditions.

For a discussion of how your EHR vendor contract should address the allocation of risk and liability between the parties, including risk and liability

[11] Pub. L. No. 114–113, div. N, tit. I.

[12] *Id.* § 405(c).

associated with patient safety, please see *Section 7 – Managing Risks and Liability*.

2.3 Ensuring Secure Implementation and Use

In addition to the safety of health IT, the security of protected health information (PHI), and the networks on which such PHI is maintained and accessed, is a shared responsibility between EHR vendors and health care provider organizations. The Health Information Technology for Economic and Clinical Health (HITECH) Act requires that business associates directly comply with the HIPAA Security Rule provisions that mandate the implementation of administrative, physical, and technical safeguards for electronic protected health information (e-PHI), and the development and enforcement of related policies, procedures, and documentation standards (including designation of a security official). Similarly, Congress, in CISA,[13] created many new initiatives to foster the sharing of cyber security threats, particularly in the health care industry. EHR vendors who manage data on behalf of their health care provider organization customers will need to participate in those efforts to improve overall health care system security.[14]

The importance of shared responsibility in ensuring the secure implementation and use of health IT is illustrated by the following example involving the installation of EHR software on computer equipment and a network that a health care provider organization maintains (a Local Area Network or LAN). The EHR vendor is responsible for developing security patches for security risks identified in the vendor's software, but you are responsible for the operational security of your environment (e.g., user accounts and monitoring, firewalls, and virus protection). As part of your operational security plan, you conduct regular security testing of your environment (e.g., "penetration tests"). As part of this testing, your security consultant identifies a vulnerability in the EHR software that could compromise the confidentiality of e-PHI. After reviewing your consultant's findings, you notify your EHR vendor to request a software patch. Your EHR contract, however, does not specify how quickly the vendor must respond and develop a patch to correct this issue, thereby presenting a significant security risk for an indefinite period of time. During this period, you may have to implement expensive compensating controls to avoid increased exposure to security attacks.

Sound security practices require a continual assessment of evolving risks, technology, and relevant issues related to information security both by you and your EHR vendor to the extent that the vendor has access to your computer network. In addition to the requirements of the HIPAA Rules, you may wish to consider including the following terms in your BAA, even though an exhaustive guide to potential security terms is beyond the scope of this guide:

- a requirement that the EHR vendor complete a security assessment questionnaire;
- a requirement that the EHR vendor obtain an independent security audit conducted by a third party and to share the results of such audit with you on an annual basis or more frequently in the event of a security breach;
- a requirement that the EHR vendor comply with your information security program, including all required network and systems security, system and application controls as may be updated from time to time, including documented policies, standards, and operational practices that meet or exceed current industry standards (e.g., NIST Common Framework);
- a requirement that the EHR vendor employ encryption methodology and secure data destruction; and
- a requirement that the EHR vendor shall comply with all applicable state and federal data security regulations.

2.4 Reporting and Discussing Problems

Despite your best efforts and your EHR vendor's best intentions, you may encounter issues during the implementation or use of your EHR that raise patient safety, security, or other concerns. To effectively respond to these issues, you may need to discuss them with other persons or organizations; you may also need to report certain issues to relevant

[13] Pub. L. No. 114–113, div. N, tit. I.

[14] *See id.* § 405(c).

organizations, such as accrediting bodies or government agencies. More generally, you may wish to share information about your EHR experiences (both positive and negative) with other industry stakeholders, such as with other health care professionals and EHR users directly, or with individuals and organizations who are engaged in the research or publication of safety-related or comparative information about health IT products and services.

(a) Disclosures Required by Law

An EHR contract should not prohibit you from reporting EHR problems, including the disclosure of confidential information, if the disclosure is required by law. You should carefully review your contract on this point.

(b) Other Reasonable Disclosures

You may need or wish to share information about your EHR experience with third parties for several reasons, including helping you to evaluate and improve the EHR or its use in your organization, enabling a consultant or reviewer to compare your EHR to another product, or supporting research on EHR quality or safety. The IOM Report[15] encouraged public reporting on comparative user experience as one means of promoting safer systems through increased transparency. Additionally, a recent report of the National Quality Forum[16] recognized that because EHRs are a rapidly evolving technology, it is vital to publicly share "lessons learned" and solutions about patient safety problems across the user community. Such information-sharing should occur in a timely manner to permit health care provider organizations to understand EHR patient safety problems that have occurred in other settings in order to prevent and mitigate similar errors.

Despite these important reasons to promote the sharing of information about EHR performance, many standard form EHR contracts limit the ability of users to voluntarily discuss problems or report usability and safety concerns that they experience when using their EHR. This type of discussion or reporting is typically prohibited through broad confidentiality, non-disclosure, and intellectual property provisions in the vendor's standard form EHR contract. Some standard form EHR contracts may also include non-disparagement clauses that prohibit customers from making statements that could reflect negatively on the EHR vendor. These practices are often referred to colloquially in the industry as "gag clauses."

Vendors include these provisions in their contracts to prevent the disclosure of any information that may either: (i) compromise their intellectual property; or (ii) reflect poorly on their EHR technology. While the protection of intellectual property and confidential information is a reasonable purpose, the use of overly-broad intellectual property restrictions to prevent or chill the reporting or discussion of performance issues, security vulnerabilities, or other problems is not. For example, some health care provider organization's complain that confidentiality, non-disclosure, or intellectual property provisions in their EHR contracts prevent them from discussing or sharing information even about relatively standard and commonplace features of their EHR, such as the publication of screen shots or interface elements that if poorly designed could lead to serious medical errors. Certain health care provider organizations have also complained that when they have alerted their vendor to major defects in the vendor's EHR software they have been required to sign non-disclosure agreements that prevent the provider organization from even disclosing the fact that a defect exists.

There is growing recognition that these practices do not promote health IT safety or good security hygiene, that EHR contracts should support and facilitate the transparent exchange of information relating to patient safety and user experiences, and that both vendors and health care provider organizations share responsibility in this area.

Given this recognition, confidentiality and non-disclosure provisions and other intellectual property protections should not be broader than reasonably necessary to protect the vendor's legitimate intellectual property interests when balanced against

[15] IOM Report, *supra* note 10.

[16] National Quality Forum, *Identification and Prioritization of Health IT Patient Safety Measures (Final Report)* (February 11, 2016) (http://www.qualityforum.org/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=81710).

patient safety and security concerns. You should review the confidentiality and non-disclosure language of your EHR contract carefully to make certain it does not prohibit your ability to conduct activities that you value and that are appropriate for improving patient safety and security, both within your organization and the provider community. For this reason, you may wish to consider negotiating a "carve out" to permit certain types of information-sharing, such as the sharing of screen shots or software documentation with third parties to whom you may wish to grant access. An example of this type of "carve out" provision is set forth below.

Some EHR contracts allow disclosure only if the EHR vendor consents and the recipient signs a reasonable non-disclosure agreement with the EHR vendor, which may be practical for some, but not all, envisaged uses. Please see *Section 6 – Intellectual Property Issues* for further discussion of this issue.

You should also ensure that any language in your EHR contract that prohibits you from disclosing the EHR vendor's confidential information is subject to standard exceptions, including the following:

- disclosures required by law or regulation, sometimes with an obligation to give the other party advance notice and the opportunity to oppose the disclosure or seek confidential treatment;
- disclosure of information that has been independently developed by the disclosing party; and
- disclosure of information that is available to the general public or has been provided separately to the disclosing party without violation of an agreement.

An example contract term relating to disclosure of certain EHR vendor information for patient safety and quality improvement purposes follows:

Example Contract Term 2

Provided, however, Customer shall have the right to disclose information relating to the Software, Services, Documentation, and EHR system to third parties for the following patient safety, public health, and quality improvement purposes: (i) sharing comparative user experiences that may affect patient care; (ii) developing best practices for EHR implementation and clinician use; (iii) reporting of EHR-related adverse events, hazards, and other unsafe conditions to government agencies, accrediting bodies, patient safety organizations, or other public or private entities that are specifically engaged in patient quality or safety initiatives; (iv) conducting research studies for peer-reviewed journals; (v) participating in cyber threat sharing activities; and (vi) identifying security flaws in the operation of the EHR that would not otherwise fall into subsection (v). The EHR Vendor hereby waives any and all claims in connection with any such disclosures.

3. SYSTEM PERFORMANCE: ENSURING YOUR EHR MEETS YOUR EXPECTATIONS

As a health care provider organization, you want your EHR to deliver improved clinical outcomes, operational efficiency, enhanced patient care, a reduction in medical errors, increased access to information, and reduced costs, among other benefits.

To achieve these goals, it is important to ensure not only that your EHR has the capabilities and features that you need but also that it will meet certain baseline performance requirements (as well as any other requirements you specify to your EHR vendor). Some baseline performance requirements you should expect your EHR to meet, and which are discussed below, include: (i) conformance with software documentation; (ii) conformance with acceptance criteria; (iii) system availability and response time; (iv) quality and timeliness of service; (v) integrity of

patient data; and (vi) compliance with applicable federal and state laws and regulations.

3.1 The Importance of Express Warranties

In a typical EHR contract, core performance requirements for the EHR are included in warranties. Warranties create legally enforceable rights that you can use to obtain the necessary performance that you desire or to pursue your vendor for damages if the vendor's performance falls short of the stated requirements. **It is critical that you ensure that all core service and performance obligations are expressly and specifically stated in your EHR contract.**

Standard form EHR contracts frequently include language disclaiming all warranties other than those expressly set forth in the EHR contract (referred to as "express warranties"). Standard disclaimer of warranty language often refers to some terms that have their origin in the Uniform Commercial Code (UCC), even though the UCC applies to the sale of goods and does not always apply to software or services.[17] These disclaimers are included in order to limit the vendor's obligations for statements that may have been made in the sales process or in its advertisements or product literature for which the vendor does not wish to be legally responsible. Such disclaimers thus limit the EHR vendor's responsibility for how or whether the software performs or meets your expectations. For these reasons, it is critically important for your EHR contract to contain appropriate express warranties regarding core EHR performance and vendor support obligations.

The importance of including appropriate express warranties is heightened by an "entire agreement" or integration provision, found in most EHR contracts, that declares the contract to be the complete and final agreement between the parties. This means that the contract itself includes all of the terms and conditions that the parties have agreed to and that no other documents, oral statements, or prior correspondence or negotiations will be binding. If your EHR contract contains an "entire agreement" or integration provision and does not contain specific express warranties, you may have difficulty enforcing promises or representations that may have been made by the EHR vendor in the sales process or in advertisements or product literature, even if you relied upon those representations in selecting the EHR vendor's product.

For these reasons, it is advisable to obtain specific express warranties regarding the specific features and functions that are important to you. In addition, you may wish to ensure that other documents that contain these terms are attached to your EHR contract and are incorporated in the contract by reference. For example, if you select your EHR using a request for proposal (RFP), then your RFP and the EHR vendor's response to the RFP, together with other sales materials, could be incorporated in the contract as an attachment or exhibit to provide a detailed description of required features and functionality.

3.2 Negotiating Express Warranties

In order to help ensure that your EHR will meet your desired performance requirements, you should negotiate certain express warranties to create legally enforceable rights with respect to core EHR system performance expectations. You should ensure that your EHR contract provides for appropriate warranties to adequately protect you in the event that the EHR vendor fails to properly implement or support the EHR. In essence, the EHR vendor's warranty obligations are your principal assurance that the system will perform in accordance with your expectations. If insufficient warranty protection is in place, the EHR vendor may not be contractually obligated to correct certain problems that occur, and you may face various risks including:

- system unavailability at critical times;
- a slow or unresponsive system that is frustrating users;
- unavailability of important reports and other data; and
- the potential for substantial unbudgeted capital expenditures to finally achieve performance expectations (which for provider-hosted and ASP model EHRs might include the acquisition or lease of additional hardware).

[17] The UCC implies certain warranties unless they are expressly disclaimed in a "conspicuous" way, such as a disclaimer in all capital letters, which is why you will see some portions of the contract written that way.

While express warranties will not necessarily ensure that you avoid the problems outlined above, such provisions afford you legal rights in the event such problems occur. Express warranties should cover the EHR vendor's standard system, customizations, and third party software that will be integral to the expected functionality of the system. Because the EHR vendor will have tested its standard system more thoroughly than it will have tested any customizations, the vendor may argue for a shorter warranty period for such customizations.

Certain key express warranties that you can consider seeking in your EHR contract are set forth below. In addition to securing appropriate express warranties, you may wish to negotiate contract terms regarding dispute resolution (see *Section 8 – Dispute Resolution: Resolving Disagreements With Your EHR Vendor*). You may also wish to ensure that your EHR contract clearly states that the EHR vendor is the single point of contact regarding performance issues. In the absence of this assurance, your vendor may outsource performance management to a third party who furnishes either a hardware or software component of the vendor's EHR. In this case, the EHR vendor and third party may each blame the other for system failures, allowing each party to claim that it is not contractually obligated to correct the problem. This could require you to pursue both parties in court and could leave you without an adequate remedy.

(a) Performance as Described in the Documentation

Software documentation is the information that describes the product to its users. It generally consists of the product technical manuals and online information (including versions of the technical manuals and help facility descriptions). The term also is sometimes used to mean the source information about the product contained in design documents, detailed code comments, white papers, and blackboard session notes. In making your selection of an EHR, regardless of whether the system is a cloud-based product or a licensed product that is locally hosted, you should ensure that the software functions in accordance with the documentation.

A common express warranty offered by EHR vendors is that the EHR will function in accordance with the EHR vendor's "then current" documentation. Before agreeing to this provision, you (or a qualified technical consultant working for you) should review the documentation and determine if it is sufficient to serve as the basis of an express warranty. Sometimes the documentation may be more like a user manual, in which case it is unlikely to include a description of the features, functions, quality, and timeliness of the EHR and so will be unsuitable. Further, you should insist that future versions of the documentation will not reduce the features and functions from those described in the documentation when the contract is signed. Vendors typically post the documentation on their company websites, which you may need to download. You also should ensure that the documentation is incorporated by reference into the contract, noting both the particular version and the date. Whether posted or not, you should consider requiring the vendor to provide you with the documentation and any updates during the term of the agreement (including access to previous versions of the documentation).

(b) Meeting Acceptance Criteria

The EHR contract should specify that the system will satisfy the acceptance criteria at all times. Acceptance criteria are the pre-agreed technical standards and requirements that the software needs to demonstrate (by way of an acceptance test) prior to being "accepted" by the health care provider organization. The purpose of acceptance testing is to identify and correct as many non-conformities as possible before the EHR goes "live" or into production. Acceptance tests are usually conducted in test environments designed to be identical, or as close as possible, to the anticipated production environment.

Such acceptance criteria should be specifically and concretely crafted with the assistance of technical personnel and documented to ensure that the EHR performs according to your expectations. The EHR vendor may argue that complete conformance with system technical specifications used as acceptance criteria is not practical, and instead will prefer to warrant that the system will "materially" or "substantially" conform to the acceptance criteria, excluding minor errors. Your counter-argument would be that "material" or "substantial" conformance is

insufficient since there may be disagreement between you and the EHR vendor with respect to how closely the vendor's performance meets the technical specifications. The vendor may still refuse to modify the language, in which case you should consult with a technical consultant to ensure that any technical specifications are drafted in sufficient detail that "material" or "substantial" conformance would meet your required needs.

If you are acquiring a certified EHR, then you should make certain that the EHR functions in your practice setting in the same manner as when tested to achieve its certification, and that you understand the vendor's obligations to maintain that certification over time. Under the ONC Health IT Certification Program rules, an EHR vendor needs to meet ongoing requirements to maintain its EHR's certification. The failure of your vendor to maintain certification and comply with other federal requirements could preclude you from meeting eligibility requirements or submitting claims for reimbursement under federal health care programs that require the use of certified EHR technology. Because these programs may be updated over time, placing different regulatory demands on you and your EHR, you should satisfy yourself that your preferred EHR vendor is contractually committed to updating your EHR to meet applicable requirements and that you understand any additional costs you may incur for such updates.

(c) Uptime Warranty and Service Level Agreements

A basic performance requirement of your EHR should be its availability. EHR data or information should be accessible and useable upon demand by your health care professionals whenever they need it. If scheduled downtime interferes with your EHR's use to any significant degree, or if more than a minimum of unscheduled downtime occurs, then the system will not only frustrate users, but also could interfere with your ability to care for patients or administer your business. Moreover, if unscheduled downtime is frequent or continuous over a period of hours or days, it can pose patient safety risks.

An uptime warranty commits the EHR vendor to limit the amount of scheduled and unscheduled downtime that the EHR will experience. An EHR vendor may be reluctant to agree to an uptime warranty, claiming that too many factors are outside of its control (e.g., the health care provider organization's network, telecommunications lines, or misuse by providers) to make such a warranty reliable. However, you can negotiate for an uptime warranty that covers only the system components and services maintained or hosted by the EHR vendor (and its subcontractors, if any) that are not affected by third parties that the EHR vendor does not control.

An uptime warranty should address the following:

- a definition of scheduled downtime;
- specifications for the maximum amount of scheduled downtime over specified time intervals;
- a guarantee of no downtime other than mutually agreeable scheduled downtime and a very low percentage of unscheduled downtime;
- a process for responding to unscheduled downtime that exceeds the agreed upon standard that will quickly uncover the causes of the failure and provide remediation;
- whether redundant back-up data and software are included and the circumstances under which they become available;
- whether uptime warranties apply when a security failure that the vendor could have prevented causes downtime; and
- a definition of when the failure amounts to a breach of contract, and the corresponding remedies for the breach.

Some EHR vendors will propose to provide "SLAs" or "Service Level Agreements" instead of an uptime warranty. An SLA specifies the level of service that a user may expect to receive from an EHR vendor by defining certain performance measures and the level of service for such measures (e.g., scheduled and unscheduled downtime, uptime). SLAs are usually presented in a separate exhibit to an EHR and stated as a standard such as "99.9% uptime." SLAs can be used to incentivize performance by providing a customer with financial credits against future service fees, in the event that an SLA is not achieved, for

example. You likely will have to negotiate with the vendor to have an SLA included in your EHR contract. The exact language used in the SLA provision also may be drafted in a manner that significantly limits your ability to claim the credit. For example, the uptime percentage may be stated as a "target" rather than a firm contractual commitment so you may find it difficult to assert a legal claim if, for example, the uptime percentage was not achieved. SLAs must be carefully reviewed in order to make certain that they provide meaningful protection.

Both legal and technical advice should be obtained in evaluating SLAs for system availability. The following are a few of the key issues that often have to be negotiated:

- Is the stated percentage appropriate for your operation? For example, if your organization is a hospital that needs its EHR to be available at all times, you may decide that you need a percentage higher than the vendor initially offers.
- As noted above, is the uptime SLA worded as a definite commitment or merely as a "target" or "objective"?
- Are there financial credits for a failure to achieve the percentage uptime and are they sufficient? SLAs often are drafted as your "sole and exclusive remedy" for the failure to achieve the uptime percentage, which means that your only recourse in the event of the vendor's poor performance would be to impose financial credits, and that you would be unable to initiate a lawsuit against the vendor for any of the damages you suffer or terminate the contract. If so, it is especially important for you to carefully consider the amount of the financial credits.
- Are there circumstances where financial credits on the contract price are an inadequate remedy? If so, what are those circumstances and when do they occur?
- Do you wish to have an exception to the "sole and exclusive remedy" so that you can terminate the EHR contract for repeated failures to achieve the uptime percentage? In other words, are there situations in which ongoing excessive downtime would not be tolerable even if you received financial credits against the fees you owe to the vendor?
- How is downtime defined? The definition and amount of scheduled downtime needs to be negotiated, because scheduled downtime will be excluded from the percentage calculation.
- How frequently is the downtime calculated? For example, is downtime calculated monthly or less frequently? Generally, a more frequent calculation will benefit you.
- Is the amount of downtime automatically calculated by the EHR and, if so, is it reported to you? It may be very difficult for you to calculate downtime.

Some vendors also prefer to use SLAs instead of warranties for overall system response time or other performance issues. The comments above may be useful in evaluating other types of SLAs, but they should always be reviewed carefully within the context of your particular needs and circumstances.

(d) System Response Time

Health care administrators sometimes receive complaints from health care professionals that EHR functionality and performance are barriers to the efficient delivery of care. Frustrations experienced by health care professionals about the amount of time they spend interacting with their EHR are compounded if the system does not respond to user commands promptly and reliably, such as when health care professionals experience a slow response time when progressing through "screen clicks" in common workflow processes. Inadequate response time also may disrupt patient care and business operations, and expose you to substantial, unbudgeted capital expenditures and project cost overruns.

The most effective way to protect yourself against these potential challenges is to obtain a response time warranty that:

- guarantees a fast, reliable EHR that meets or exceeds user expectations;
- specifies a mutually agreeable method for calculating response time (e.g., measuring

response time as an average of all transactions over a specific period of time, such as a month, with financial credits against future fees if the agreed upon average is not achieved);

- describes a process for responding to response time failures; and
- defines when the response time problem amounts to a breach of contract, and the corresponding remedies for the breach.

Even if your vendor agrees to provide a response time warranty, it may seek to limit the scope of the warranty in several respects.

First, the EHR vendor may seek to establish parameters governing when the warranty applies. For example, the vendor may wish to limit the warranty to certain transaction or volume levels or to the use of your EHR with the vendor's own products or with third party products approved by the EHR vendor. The vendor may seek this limitation because it cannot ensure the response time of unapproved third party products or sources of information over which it has no control.

Second, the EHR vendor may seek to limit your remedies for a breach of the warranty to either undertaking "software tuning" or similar measures at its own expense, or to a combination of software tuning and other corrective measures. You should object to this limitation since it may not be a sufficient remedy because it may not correct the problem.

Third, the EHR vendor may seek to limit the warranty to a "snapshot" in time (e.g., completion of implementation) or establish a specific time limit on the duration of the warranty following completion of implementation. You also may wish to object to this limitation.

You should consult with your legal counsel and a technical expert to determine whether any limitations discussed above are acceptable in light of your intended uses of your EHR, including any needs you may have to use third-party applications or services, and to develop an appropriate response time warranty. For a further discussion of issues relating to interoperability, please see *Section 5 – Fostering Interoperability and Integration*.

(e) Integrity of Patient Data

You will need to rely on the information in your EHR to deliver safe and effective care to patients, to comply with applicable regulations, including the HIPAA Security Rule, and for other critical aspects of your health care operations and business.[18] For these reasons, the integrity of data within your EHR will be important to you.

EHR-related errors can result in data being lost or incorrectly entered, displayed, or transmitted, leading to loss of information integrity. For example, the use of voice recognition systems without a process in place to verify the accuracy of the output compared to the input can result in documentation errors. Similarly, errors in patient identification could cause information to be documented in the wrong medical record, thereby affecting clinical decision-making and jeopardizing patient safety. Such data integrity issues have the potential to lead to errors that endanger patient safety or decrease the quality of care. Additionally, data integrity issues may occur from poor security practices, inappropriate use of "copy and paste" functionality, or misuse of templates originally designed for documentation efficiency, which could lead to allegations of health care fraud and abuse.

An example of a contract term that imposes appropriate obligations on an EHR vendor to assure the accuracy and integrity of patient data is set forth below. This example term assumes that the EHR is delivered under a provider-hosted model. If the EHR is delivered under a cloud-based model, the responsibility for protecting and backing up data would need to be allocated to the vendor.

[18] The HIPAA Security Rule requires covered entities and business associates to conduct a security risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information and correct identified security deficiencies. *See* 45 C.F.R. § 164.308(a). The Medicare and Medicaid EHR Incentive Programs include requirements for conducting security risk analyses and implementing security updates as necessary, and correcting identified security deficiencies. *See, e.g.*, 42 C.F.R. § 495.22(e)(1). Under the 2015 Edition certification criteria, certified health IT must "permit an identified set of users to access electronic health information during an emergency." *See* 45 C.F.R. § 170.315(d)(6).

Example Contract Term 3

The EHR Vendor shall employ appropriate system testing and quality assurance measures to ensure the accuracy and integrity of all patient data, financial, and other information within the EHR system. The EHR Vendor further shall ensure that: (i) the EHR system data or information shall not be accessed, altered, or destroyed in an unauthorized manner; (ii) the EHR system employs available matching technology and capabilities to accurately match data to a particular patient consistent with commercially reasonable standards; and (iii) implementation of appropriate physical, administrative, and technical safeguards to ensure the privacy and security of all data and other information within the EHR system.

The Customer shall be responsible for: (i) the accuracy and adequacy of patient data initially entered by Customer in the EHR system; (ii) use of proper procedures and input of correct patient data, financial, and other information; (iii) protecting and backing up the patient data, financial, and other information entered and stored in the EHR system; and (iv) promptly notifying EHR Vendor of any data errors reported to it that cannot be corrected through the Vendor's existing automated processes.

(f) Quality and Timeliness of Service

Your EHR vendor will provide certain implementation and maintenance services as part of the EHR contract. Consequently, your EHR vendor should make warranties concerning the quality and timeliness of those services. An example of this type of provision is set forth below:

Example Contract Term 4

The Services provided hereunder shall be performed in a timely and professional manner and consistent with applicable federal and state laws and regulations by EHR Vendor's project personnel and permitted subcontractors having the level of skill sufficient to fulfill all the requirements of this Agreement, including all of the Customer's policies and procedures relating to safety and personal conduct. The performance of the Services shall in no manner and to no extent cause Customer to suffer any permanent and irrevocable loss, corruption, alteration, or destruction of Customer's data, hardware, or software ("Customer Data") with which EHR Vendor interacts in the performance of the Services, or cause any failure in security. In the event of any loss, corruption, alteration, or destruction of Customer Data, or the unavailability of Customer Data, regardless of whether permanent and irrevocable or otherwise, EHR Vendor shall, at its sole expense, recover, or attempt to recover (in the case of permanent loss), the Customer Data within a mutually agreed upon timeframe.

(g) Non-infringement of Third Party Intellectual Property Rights

If your EHR vendor does not have ownership or license rights to support its grant of a license to use the software, then you may be exposed to a lawsuit for infringement of another person's intellectual property rights, exposed to monetary damages, and ultimately prevented from using the disputed software. This could significantly impair, or completely prevent, your ability to use the entire system to administer patient care and meet business needs, especially if the software is integral to the overall functionality of the EHR. Your vendor should warrant that it is the owner of, or has the right to license, all current and future intellectual property that may be included in or required for your use of the EHR and any related services provided under the contract. An example of this type of provision, suitable for a provider-hosted EHR, is set forth below:

Example Contract Term 5

EHR Vendor represents and warrants that it either has the full right and title to the licensed Software and all related intellectual property as may now or in the future exist, or full rights to license the Software and all related intellectual property for use by Customer under the terms of this Agreement. EHR Vendor shall not place on the Software any liens, security interests, or other encumbrances that would in any manner

affect Customer's rights under this Agreement. EHR Vendor further warrants that the Software shall not violate or in any way infringe upon any rights of third parties including, but not limited to, any property, contractual, employment, proprietary information, or non-disclosure rights, or any copyrights, patents, trademark, trade secrets, or other proprietary rights.

(h) Compliance with Applicable Laws and Regulations

The EHR contract should address new releases and enhancements to the software or cloud service that may be required in order to permit you to comply with changes to applicable federal and state laws and regulations (e.g., certification requirements, HIPAA Rules, and the Meaningful Use requirements). An example of this type of provision for use with respect to a provider-hosted EHR, which likely will need to be customized to meet your specific needs, is as follows:

Example Contract Term 6

The Software initially delivered to Customers shall, if properly used in accordance with the Documentation, permit Customer to comply with applicable federal and state laws and regulations which fall within the scope of the Software's functionality described in the Documentation as of the effective date of this Agreement. During the post-implementation maintenance period, the EHR Vendor shall provide Customer on a timely basis and at no additional cost, other than the software maintenance fees set forth herein, new releases and enhancements to the Software which, if properly used in accordance with the Documentation, shall permit Customer to comply with any changes to federal and state laws and regulations which: (i) are in effect at the time of delivery of those new releases or enhancements; and (ii) fall within the scope of the Software's functionality described in the Documentation.

If you are procuring a cloud-based EHR, you will need to ensure that your EHR contract clearly specifies that the "Services" to be provided, along with new releases and enhancements, permit you to comply with applicable federal and state laws and regulations throughout the term of the EHR contract.

Some EHR vendors may include in their base fees the vendor's cost of developing and implementing new releases and enhancements to enable you to comply with changes to applicable federal and state laws and regulations. However, some vendors may require you to pay for certain regulatory updates if, for example, the vendor's customer base is not significantly affected by the regulatory update, such as state specific laws and regulations, which could be very costly. In such instance, the following language, suitable for a provider-hosted EHR, may be useful in minimizing the cost of such updates:

Example Contract Term 7

Provided, however, that if any such Regulatory Updates require significantly new features, functionality or extraordinary additional software development efforts beyond that historically and customarily expended by EHR Vendor in providing Software Maintenance Services, then EHR Vendor may charge, and Customer agrees to pay, for such efforts at a price not to exceed Customer's pro-rata share of EHR Vendor's actual costs of developing such Regulatory Update (such pro-ration to be based directly on the total number of Customers that have licensed the affected Software and are affected by the Regulatory Update).

(i) Post-implementation Support and Maintenance

Any express warranty relating to the EHR vendor's obligation to provide maintenance and support should be in effect throughout the entire contract term. If your EHR contract includes maintenance services to be performed beyond the acceptance date (or continuing past the duration of the performance warranty period), then the EHR vendor also should warrant that such services will be performed in a timely manner. An example of this type of provision, that has been prepared on the assumption that the EHR in question is provider-hosted, is as follows:

Example Contract Term 8

Following Customer's Acceptance of the Software and during the term of Customer's support and maintenance agreement, such Software (and each portion or component thereof) shall be free of material defects and shall operate in all respects in conformance with the Acceptance Criteria. In the event that Customer notifies the EHR Vendor of any defects, malfunctions, or nonconformities during such period, then the EHR Vendor shall use its best commercial efforts to correct any such nonconformities, and shall undertake corrections in accordance with the Escalation Support Schedule, at no additional cost to Customer. The foregoing warranty shall not apply if and to the extent a nonconformity with such warranty is directly caused by: (i) Customer's material failure to operate the Software in accordance with the Documentation provided by EHR Vendor; (ii) Customer's material modification or alteration of the System, or any Software, without EHR Vendor participation or approval; (iii) use of the Software by Customer in conjunction with third-party hardware or software that EHR Vendor has not agreed is compatible with the Programs, which agreement shall not be unreasonably withheld or delayed; and (iv) malfunctions in Customer's computer hardware. This warranty shall be extended for so long as the post-acceptance support and maintenance obligations of the EHR Vendor under this Agreement remain in effect.

In a cloud-based environment, post-implementation support and maintenance typically would be bundled with the general service obligations of an EHR vendor.

(j) Viruses, Keylocks, and the Like

The EHR vendor also should warrant that any software provided to you is free from any viruses and that the system does not contain any keylocks, "back doors" or "time bombs." This issue is discussed in further detail in *Section 4 – Data Rights: Managing and Safeguarding Your EHR Data*.

4. DATA RIGHTS: MANAGING AND SAFEGUARDING EHR DATA

Having reliable access to clinical and business data and being able to provide patients with electronic access to their health information are among some of the most compelling benefits of an EHR. Yet standard form EHR contracts may not include terms that help ensure the availability and integrity of data in your EHR, and may even seek to limit your rights to access, control, or use data for certain purposes. This may result in significant risks that you may not anticipate. For example, your EHR vendor may:

- seek to commercialize protected health information (PHI) that has been de-identified, or other data, such as information about your clinical and business operations, in ways that you or your patients find unacceptable;
- fail to take reasonable steps to protect, back up, and recover your data in the event of a disaster, outage, security incident, or other unexpected event involving a cloud-based EHR; or
- stop performing services—or design the system or software to automatically stop functioning—if you fail to make payments, even if due to a good faith dispute.

While your Business Associate Agreement (BAA) with your EHR vendor may govern certain aspects of these and other issues, it is important to also understand and negotiate appropriate data rights and related terms as part of your EHR contract. As discussed in this *Section 4*, these terms can help you to avoid potential problems such as those described above that could be harmful to your business, patients, or reputation, and help assure that your data is available when and where you need it.

In addition to the topics discussed in this section, your ability to access and use EHR data may be affected by issues regarding interfaces and the interoperability of data. These issues are addressed in *Section 5 – Fostering Interoperability and Integration*.

4.1 Controlling EHR Data

Many standard form EHR contracts grant vendors very broad rights to use and commercialize data captured in or created by an EHR. For example, your vendor may claim the right to de-identify and sell your patients' PHI to third parties, or to use or commercialize other data about your clinical and business operations without your permission or without masking your identity. While you may be open to participating in research activities or comfortable with your clinical and operational data being used for benchmarking or other defined purposes, it is prudent to ensure that your EHR contract puts you in a position to control how and when your data is used by your EHR vendor.

The most important first step to mitigate these risks is not to grant your vendor more rights to EHR data than is necessary for it to perform the services required under your EHR contract. At a minimum, your EHR contract should clearly state that—*as between you and the EHR vendor*—all data stored in, created by, or received by the EHR, including PHI of patients and all information about your organization, is your sole and exclusive property. Ensuring that your EHR vendor does not own the information in your EHR ultimately benefits your patients. If you don't own and control the data in your EHR, you limit your ability to act as a custodian of your patients' health information, or to participate in public or private research activities that rely on EHR data (typically in de-identified form). Example contract language for this purpose is set out below, but it is not a legal pronouncement about any claim of ownership your patients may have under law and does not control whether you or your patients ultimately own the PHI. This example contract term also includes a general prohibition against the EHR vendor de-identifying PHI, which is discussed below.

Example Contract Term 9

As between EHR Vendor and Customer, Customer is and shall continue at all times to be the sole and exclusive owner of all PHI and all other data and information provided by Customer or which EHR Vendor develops or receives on behalf of Customer or has access to in connection with this Agreement (collectively, the "Customer Data"), and all intellectual property rights in or with respect to any or all of the Customer Data. EHR Vendor may use or disclose the Customer Data only to the limited extent necessary to perform its obligations under this Agreement. Without limitation of the foregoing, EHR Vendor shall not create any de-identified information from the PHI included in the Customer Data, shall not use or disclose any of the Customer Data for benchmarking or other comparisons, and shall not create any derivative works using any or all of the Customer Data unless expressly agreed herein.

Of course, your EHR vendor will need some rights to access and use the information in your EHR to perform the required services, and the above model term grants it these rights (with such rights subject to the terms of your BAA with your EHR vendor and the HIPAA Rules). You may decide to grant your vendor additional data rights for certain **limited** purposes, as discussed below. Such additional rights would operate as limited exceptions to the general rule that the EHR vendor can only use your EHR data for the services it is obligated to perform.

(a) Granting Data Rights to the EHR Vendor to Perform Additional Services

Some health care provider organizations give their EHR vendor limited rights to use and possibly disclose PHI and other data created and stored in the EHR for the purpose of performing additional services for the health care provider organization or on the health care provider organization's behalf. These additional services may include: (i) reporting to public health authorities; (ii) analyzing data to improve quality (e.g., reduce hospital readmissions and coordinate and close gaps in care); or (iii) creating a de-identified version of the data for the health care provider organization's use. Under these arrangements, the EHR vendor would be a business associate with respect to the PHI involved, so the uses and disclosures should be subject to a BAA. **You cannot give the EHR vendor more rights than you have under HIPAA as well as other federal and state laws and regulations, so the EHR vendor's rights should be drafted with those limitations in mind.**

(b) Granting Data Rights to the EHR Vendor for Uses Other than Performing Services

EHR vendors often seek broader rights to use PHI and other health care provider organization data, including the right to de-identify the PHI in accordance with the HIPAA Rules and to use the de-identified data for the EHR vendor's purposes. Although granting the right to de-identify PHI in accordance with HIPAA and thereafter use the resulting data for the vendor's purposes would not violate HIPAA, many other uses of data by an EHR vendor might be deemed a sale of PHI in violation of HIPAA. You should make sure that any other proposed use of PHI does not violate HIPAA before agreeing to it.

Many health care provider organizations are unwilling to grant vendors the right to create and use de-identified data from PHI. The reasons for refusal are varied but may include concerns that de-identification in accordance with HIPAA may not reduce the risk of re-identification to zero in all cases, or fears about damage to a health care provider organization's reputation with its patients.

Even if granted, you may insist that your EHR vendor agree that any use of the de-identified data should be limited so that third parties are not able to identify you or any of your health care professionals. You can also require that if the EHR vendor wants to create and use de-identified data sets, it indemnifies and holds you harmless for any legal liability that arises out of the vendor's use of those data sets.

4.2 Ensuring that Data is Available Despite Certain Emergencies

There is a risk that a cloud-based EHR could become unavailable due to a failure of the vendor's software or infrastructure, unplanned outages by a third party hosting service or utility company, or a natural disaster, civil unrest or other problems. You also face these risks if you license and operate the EHR software yourself. In this case, your EHR contract may impose obligations on your vendor to provide technical assistance in certain circumstances, but it will not typically address service availability and emergency response issues if emergencies arise. In these circumstances, you can (and should) develop your own disaster recovery plan consistent with the principles discussed below and the HIPAA Security Rule requirements.

You might expect that a cloud-based EHR vendor would be responsible for data backup and for switching operations to an alternative location in the event of an emergency, but standard form EHR contracts often fail to address this situation and some even disclaim the vendor's responsibility for loss or unavailability of data. They also typically provide that the EHR vendor is not liable if it is unable to perform due to a variety of factors beyond the EHR vendor's control. These are sometimes referred to as "force majeure events"—for example, tornados, fires, floods, acts of war, civil unrest, terrorism, strikes, etc. "Force majeure" language could be interpreted to mean that the EHR vendor does not have responsibility to operate the EHR under these circumstances, contrary to your expectations.

A full discussion of the obligations of the EHR vendor under the HIPAA Security Rule is beyond the scope of this guide. The discussion below is intended to help you focus on the extent to which you as a health care provider organization have delegated certain of your HIPAA Security Rule responsibilities to the EHR vendor and whether it has provided you adequate protection with respect to certain aspects of those obligations. You may have additional rights under the BAA which are not addressed below.

In a cloud-based EHR, you should carefully assess your preferred EHR vendor's approach to data backup and disaster recovery. You should also ensure that your EHR contract contains terms that provide your organization with sufficient protection in the event of an unplanned outage or other disaster and will help you continue to comply with the HIPAA Security Rule and The Joint Commission standards, if applicable. These risks are usually addressed by the EHR vendor agreeing in an EHR contract to maintain a disaster recovery plan that includes periodic backups of data and software applications and detailed arrangements for the operation of the EHR at another site in the event of a major problem with the primary site. The requirement to maintain a disaster recovery plan will also be addressed in your BAA.

Your comfort level with an EHR vendor's data backup and disaster recovery plan should be an important factor in selecting a cloud-based EHR because of its potential impact on patient care and safety, continuity of your business operations, and compliance with applicable standards. You may need help from a security professional to determine whether the frequency, extent, and storage of the backups and the overall disaster recovery plan give you sufficient protection. Common elements of a disaster recovery plan would typically include the following:

- maintenance of a "hot site" or a "cold site" for the EHR services. A hot site typically is a mirror image of the main processing operation that maintains the same data through frequent backups or real-time synchronization so that service could be restored in hours or a few days. By contrast, use of a cold site may result in a slower restoration of services because, although there are arrangements in place for the use of computers, space, and storage of media, the cold site operations would not be implemented until the disaster was declared. There are also "warm site" approaches that are in between these two alternatives;
- a backup site in a location that does not present the same risks of natural disaster, civil unrest, etc., as the primary site;
- rules that specify what circumstances constitute a disaster and who can declare it;
- assurances that all customers of the EHR vendor are treated the same in the event of a disaster, or that you would receive some priority over other customers;
- a commitment to recover data and restore operations within a specific period of time; and
- a methodology to validate the integrity of the data recovered.

Assuming that you have reviewed and are comfortable with your preferred EHR vendor's disaster recovery plan, typical contract protections for this type of risk include the EHR vendor committing to: (i) maintain and implement a formal disaster recovery plan in order to restore functionality within a stated period of time; (ii) update and test the plan annually; (iii) share the disaster recovery plan and test results with you before the contract is signed and promptly share the results of future tests and any updated plan; (iv) promptly correct any problems revealed by the tests; and (v) give you prompt notice of any changes in the disaster recovery plan. The following is example contract language for these protections:

Example Contract Term 10

EHR Vendor shall maintain (and cause any third party hosting company that it uses to maintain) a disaster recovery plan that satisfies all HIPAA Security Rule requirements and implement it when services are unavailable (or likely to be unavailable) for more than ___ hours in any ___ day period. EHR Vendor shall update and test the disaster recovery plan at least once every twelve (12) months. EHR Vendor will provide Customer with a copy of the results of such testing within thirty (30) days after it has been conducted and shall promptly remediate any problems disclosed in such testing. EHR Vendor shall also provide Customer with a copy of updated versions of the disaster recovery plan of the EHR Vendor (and any third party hosting company that it uses) within thirty days after changes are adopted, or within in 5 days of Customer requesting a copy. Customer shall be free to share the disaster plan with any government agency with jurisdiction to request a copy from Customer.

You may also need to negotiate the details of periodic backups including the frequency, the scope of the backup, and the location for storage of the backup copies.

As noted above, typical "force majeure" language could be interpreted to mean that the EHR vendor is not responsible for loss of service due to natural disasters which could undercut the protection that you tried to obtain by including disaster recovery provisions. You may want to be able to terminate the EHR contract early if the force majeure event continues for more than a stated period and receive a

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 labor, energy, raw materials or supplies, war, terrorism, riot, act of God, or governmental action (each a "Force Majeure Event"); provided, however, that EHR Vendor may not rely on this provision if it has not maintained or implemented the disaster recovery plan and procedures as required by this Agreement. Customer shall not be obligated to pay any fees or other amounts for periods during which 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 otherwise due hereunder for future services if a Force Majeure Event affects EHR Vendor's performance hereunder in any material respect for more than ___ days. EHR Vendor shall also refund any amounts which were paid in advance for services that were not provided due to the Force Majeure Event and for any services that will not be performed in the future if this Agreement is terminated due to a Force Majeure Event.

Another important protection is an "uptime" 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 3 – 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 disputes (sometimes referred to as a "kill switch").[19] 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. This type of conduct by an EHR vendor obviously 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 portions thereof) do not and shall not in the future contain any timer, clock, counter, keylock, or other limiting design, routine, device, or other mechanism that causes or could cause the Software, data, or Services (or any portion thereof) to become erased, inoperable, impaired, or otherwise incapable of being copied or used in the full manner for which it was designed or required to be provided hereunder (collectively, "Disabling Technology"). In the event of a breach of this provision, the EHR Vendor shall not use or permit any of the Disabling Technology to be used and shall, at the EHR Vendor's sole expense, promptly remove the Disabling Technology and take all other action necessary to comply with this provision.

You may also want to propose language requiring both parties to continue to perform their obligations in the event of a dispute as discussed in *Section 8 – Dispute Resolution: Resolving Disagreements With Your EHR Vendor*.

[19] *See* ONC, Report to Congress on Health Information Blocking (April 2015), available at https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf. In particular, Scenario 3 in Appendix A – Information Blocking Scenarios, is an example of circumstances under which the operation of a "kill switch" was deemed to constitute information blocking.

4.4 Patient Access to Electronic Health Information

Under HIPAA and some federal payment rules, you are required to provide patients with copies, including electronic copies, of health data about them. You are required to allow patients to transmit copies of that data to any third party they choose. You are also required to allow them to request that transmission by unsecured email. Patients can also authorize a family member, a friend, or even a software application of their choosing to exercise their access rights for them. For more information see the HHS Office for Civil Rights' (OCR) guidance on individuals' right under HIPAA to access their health information.[20]

Patients have increasing expectations about the prompt availability of this information, and while federal regulations generally give a deadline in which to supply a copy, OCR recognizes that electronic health information technology may enable "almost instantaneous or very prompt electronic access."[21] Patient access is also recognized as vital to patients becoming more involved in their own care and is a key measure of performance under existing and proposed government and private sector programs that link reimbursement for health care services to quality and value.

For these reasons, it is important that your EHR contract address how the vendor will support and assist you in fulfilling these responsibilities.

(a) Individual Right of Access Under HIPAA

If you are a health care provider organization subject to HIPAA, then you must provide patients with access to their PHI maintained in your EHR in any readily producible form and format (including an electronic format) that a patient requests.[22] In addition, you must comply with a patient's signed written request to transmit electronic PHI to any third party whom the patient designates and in any readily producible form and format that the patient requests (and that would not present an unacceptable level of security risk to the PHI in your EHR). OCR has clarified that entities covered by HIPAA are expected to be able to transmit PHI electronically via e-mail and using the capabilities of certified EHR technology.[23]

Your EHR contract should ensure that you will be able to comply with these requirements. An example of contract language to help address this requirement is as follows:

Example Contract Term 13

The EHR Vendor represents and warrants that use of the EHR allows Customer to comply with the provisions of 45 C.F.R. §164.524(c)(2) by making all PHI contained within the EHR as a designated record set readily producible to patients, or patients' designees, in electronic versions and in hard copy, all in forms and formats acceptable to the Customer, and further represents and warrants that if the EHR system is certified pursuant to the 2014 Edition or any subsequent Edition of Certification Criteria issued by the Office of the National Coordinator for Health Information Technology, the EHR system enables Customer's patients to view, download, or transmit the required types of data without special effort and without cost to the patient.

(b) "Meaningful Use" and Other Reimbursement Programs

Separate from the HIPAA requirements described above, health care reimbursement rules under federal, state, and commercial programs may require or provide incentives for you to make information in your EHR accessible to patients (and other persons of their choosing) in a variety of electronic forms and formats. Importantly, the Medicare and Medicaid EHR Incentive Programs (commonly referred to as the "Meaningful Use" programs) contain several objectives and measures related to patients' access to

[20] *See* HHS Office for Civil Rights, Individuals' Right Under HIPAA to Access Their Health Information, *available at* http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html (last accessed Sept 14, 2016).

[21] Id.

[22] If the PHI is not available in the requested form and format, it may be provided in a readable electronic format as agreed to by the provider and the patient. *See* 45 C.F.R. § 164.524(c)(2)(i).

[23] *See* HHS Office for Civil Rights, *supra* note 20.

their electronic health information. In addition, for eligible clinicians, the Meaningful Use programs will be combined with other federal quality-based payment programs under a single reimbursement framework that transitions from fee-for-service to value-based payments, as required by the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA).[24] As currently proposed, eligible clinicians participating in the Merit-based Incentive Payment System (MIPS) would be required to meet objectives and measures related to patient electronic access and patient engagement that will require, among other things, providing patients (or their authorized representatives) with timely access to view online, download, and transmit their health information, and enabling them to access this information using an application of their choice that is configured to meet applicable ONC certification criteria.[25] While the discussion and example contract term below focus on the existing Meaningful Use requirements, you should be aware of and ensure that your EHR contract addresses your need to comply with other applicable programs and requirements, including increasing expectations for providing patients with timely and robust access to information about them maintained in your EHR.

The Meaningful Use requirements are detailed, so you should first seek to understand them before evaluating whether a specific EHR will function effectively with your workflow in order to achieve all of the relevant objectives and measures. Many health care provider organizations have found it necessary to change their workflows in order to work effectively with a new EHR and achieve Meaningful Use. You should also be aware that the Meaningful Use requirements vary by stage. A description of the requirements for each stage is beyond the scope of this guide. The discussion below is intended to provide only a few examples of required functionality that are important in selecting an EHR.

One of the Meaningful Use objectives requires a health care provider organization to give patients the ability to view online, download, and transmit their electronic health information within time periods that are much shorter than those required by HIPAA. You should be aware that your workflow may need to be reconfigured to meet the applicable deadlines. For example, you may need to expedite the review of test results that convey an adverse diagnosis to allow a physician the opportunity to personally convey this information to the patient before posting the test results to the patient portal within the Meaningful Use time periods.

Another Meaningful Use objective requires that a minimum number or percentage of patients do in fact view, download, or transmit their health information. This may be challenging for some health care provider organizations because it depends on action by the patients themselves. Choosing an EHR with "patient friendly" electronic access and an easy-to-use interface, may help you satisfy this requirement.

In an effort to increase care coordination, there is also a Meaningful Use requirement that a certain percentage of patients either view, download, or transmit their health information to a third party or access their health information through an API (application programming interface) that can be used by applications chosen by the patient and configured to the API in the health care provider organization's certified EHR. There are also requirements regarding the use of health information exchanges and public health and clinical data repository reporting.

These are only a few of the many requirements that you should consider in selecting an EHR because your EHR's functionality will be critical to your ability to achieve Meaningful Use. In order to satisfy the Meaningful Use requirements, a starting point in your evaluation of potential EHRs should be the use of certified EHR technology that is current with the requirements of the applicable ONC Edition (e.g., 2014 or 2015) of certification criteria (see Part A, section (iv) of this guide for more information about certification requirements and the importance of using a certified EHR). However, an in-depth review of certified EHR technologies should not be overlooked because there are significant differences in their functionality. You should also be aware that under the ONC Health IT Certification Program rules, a certification issued for a health IT product is not perpetual and that an EHR vendor needs to meet

[24] Pub. L. 114–10.

[25] 81 Fed. Reg. 28227.

ongoing requirements to maintain its EHR's certification. The loss of certification by your EHR would have a significant impact on your organization, including the ability of your organization and/or its health care professionals to comply with Meaningful Use or other federal health care program requirements.

As noted above, in addition to the Meaningful Use requirements, you should ensure that any contract term also addresses requirements under other applicable reimbursement programs, such as those established pursuant to MACRA.

An example of general language to help assure that the EHR will enable the health care provider organization to comply with Meaningful Use requirements, including data access and management criteria, is provided below. This example assumes that the health care provider organization is an Eligible Hospital seeking Medicare incentives, the EHR is hosted and supported by the EHR vendor, and the EHR is a "Health IT Module" that has been certified to the ONC's 2015 Edition certification criteria as necessary to comply with the Meaningful Use rules. This language should not be used without customizing it to your particular situation and adding appropriate definitions. In particular, this language would need to be adapted for use by a physician practice or other provider organization that is not a hospital. It would also need to be modified to address compliance with requirements of other reimbursement programs, separate from Meaningful Use, such as programs established pursuant to MACRA.

Example Contract Term 14

1. As part of its standard support and without any additional license, implementation, support, or other fees or expenses, EHR Vendor will provide the following to Hospital so long as Hospital is receiving software maintenance under this Agreement:

(a) All versions of the Software necessary to satisfy all requirements in order to be Certified EHR Technology for use by Hospital and, at Hospital's election, its non-employed medical staff, so that they can each qualify to receive all of the Medicare incentives available under HITECH beginning on _____ __, 201_ and will not be subject to any reduction in reimbursement as a result of a failure to use Certified EHR Technology as a "meaningful user." Such software shall be provided: (i) with respect to the current definition of Certified EHR Technology, at least _____ months prior to _____ __, 201_ [insert date used above]; and (ii) if the definition of Certified EHR Technology is revised thereafter or a different definition is used under successor laws or regulations, an updated version of the Software that satisfies each such revised definition at least ____ months before the revised definition becomes effective. Such new versions may be referred to as "Certified EHR Versions."

As used herein, the terms "Certified EHR Technology," "Health IT Module," and "meaningful user" each have the respective meanings assigned to such terms in HITECH (and any subsequent amendments thereto) and in the regulations promulgated from time to time pursuant to HITECH, including whatever are then the most recent versions of HITECH and such regulations or any successor laws and regulations (the "Current Requirements").

(b) All implementation, training, data conversion, and other services that may be necessary or appropriate to reasonably assist Hospital in implementing each of the Certified EHR Versions that Hospital may, in its discretion, elect to implement, and in becoming a "meaningful user."

2. EHR Vendor hereby represents and warrants that as of the date of this Agreement, Version ___ of the Software being licensed hereunder has been certified as a Health IT Module pursuant to the Current Requirements;

3. EHR Vendor hereby agrees that it shall take all action necessary to assure that the representations and warranties set forth in Section 2 above shall remain true and correct with respect to Version ___ and all future versions of the Software at all times during the period in which Hospital is entitled to receive software maintenance under the Agreement.

5. FOSTERING INTEROPERABILITY AND INTEGRATION

Even if you rely primarily on one vendor for all of your health IT needs, your EHR will still need to be "interoperable" with other IT systems or applications to deliver the functionality you expect and may need in the future. Two systems are interoperable if they can exchange information and understand and use the information exchanged without special effort on the part of the user.[26]

This ability to communicate seamlessly and to integrate information from other systems is necessary to achieve many of the most compelling benefits of EHRs, such as obtaining quick access to patient information, streamlining clinical and administrative functions, identifying and closing gaps in patient care, and helping patients understand the totality of their health. Moreover, under new alternative payment models that emphasize outcomes and value, you will likely need to integrate data from a wide range of sources outside your health care provider organization or network. These may include data from medical and health tracking devices, claims databases, clinical registries, community platforms for population health management, and health information exchanges, among other sources.

In recent years, health IT products, including EHRs, have become more interoperable, especially for certain use cases such as e-prescribing and immunization reporting. However, work remains to fully realize the goal of widespread and impactful interoperability. You should be aware that not all EHR vendors offer the same capabilities for sharing, receiving, and integrating data with other sources. As a result, a vendor's willingness to support your need to exchange and integrate data may be a key factor in deciding on your preferred EHR. Your EHR contract should bind the EHR vendor to the promises that it made to you about interoperability and integration, and the costs and timelines associated with achieving your desired level of interoperability.

[26] *See* ONC, *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap version 1.0,* https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf (October 2015).

5.1 Integrating Your EHR with Your Existing Systems

Many health care provider organizations use software and services from different vendors for various parts of their operations such as billing, scheduling, labs, radiology, and EHRs. Often these systems and services are not initially interoperable, meaning that the EHR vendor will need to do extra work to allow the systems or services to communicate and exchange data with each other and to use the information that has been exchanged. Because the manual transfer of information is inefficient and may introduce errors, this "extra work" usually involves the use of technical solutions that enable your EHR to receive and incorporate data from external sources and to transmit data in a format that can be used by other health IT systems and applications. These solutions vary and may include, for example: (i) "point-to-point" interfaces used to convert or map data between incompatible systems or modules; (ii) "data feed" or "batch export" capabilities in an EHR that allow data to be exported at automated intervals in a standard format; and (iii) service-based architectures that allow other health IT systems and applications to connect to and interact with data in an EHR via application programming interfaces (APIs). For the purposes of this *Section 5*, the term "interface" refers broadly to any of these and other interoperability solutions.

It is helpful to determine early in the selection process whether a particular EHR will efficiently interface to all other systems and services you currently use, or propose to use in the future, and to obtain the EHR vendor's commitment to provide the initial interfaces and keep them up to date. If the EHR vendor has not previously interfaced to the specific third party software and services you need, it may be costly and time consuming to develop a new interface. As a result, whether an EHR has pre-existing interfaces to your other software and services may be an important consideration in your choice of EHR, as may be an EHR vendor's proven ability to efficiently develop and support additional interfaces at a reasonable cost. Even pre-existing interfaces may require substantial customization and may be the subject of additional fees, so you should make sure they are covered in the fees quoted by the EHR vendor.

Any interfaces that your EHR vendor develops and/or implements for you should be included in the definition of the EHR software or services so that the warranty and support provisions of the EHR contract apply to the interfaces. Standard form EHR contracts seldom address interfaces in depth so you may need to negotiate to obtain the EHR vendor's promise to keep the interfaces up to date as changes occur in the EHR technology itself and in the third party software or services to which your EHR is interfaced. If the EHR vendor resists making this commitment, you may wish to stress the importance of this issue in your selection of an EHR because it will need to work effectively with other technology during the entire term of the EHR contract and respond to the rapidly changing health care environment.

Set out below is an example of EHR contract language requiring your EHR vendor to provide and maintain specific interfaces. You should also obtain technical input on this language and on the exhibit to your EHR contract that will list the relevant third party software or services and the specifics of how the data should be transferred using the interfaces.

It is also important to have a procedure to monitor whether interfaces are working correctly, especially after upgrades or other modifications of any of the software or services involved. A failure to update interfaces when necessary could introduce security risks that, if not assessed and addressed, could violate the HIPAA Rules; and interfaces that do not operate correctly can present serious risks to patient safety. *See Section 2 – EHR Safety and Security: A Shared Responsibility* and *Section 7 – Managing Risks and Liability* for a discussion on how to manage these risks.

Example Contract Term 15

The EHR system provided hereunder includes interfaces to each of the third party software and services listed on Exhibit __. The interfaces automate the bi-directional transfer of data between the EHR and the third party software/services, all as further described on Exhibit __. The interfaces listed on Exhibit __, all future interfaces provided under this Agreement, and all updates to the current and future interfaces, shall transfer data without loss of or changes to information content, and without losing, deleting, modifying, or corrupting, or otherwise compromising any of the coded or free-text data to be transferred.

All interfaces and updates provided under this Agreement shall have been thoroughly tested and all interoperability, security, or other issues resolved before they are implemented for Customer. At Customer's request, Customer may participate in the acceptance testing. Customer shall also have the right to prohibit implementation of any initial or updated interface without its prior written approval; provided, however, that such approval shall not be unreasonably withheld or delayed if Customer has received documentation establishing that reasonable acceptance testing has been successfully completed.

Prior to implementing any update or other modification of the EHR, the EHR Vendor shall consult with Customer and revise the existing interfaces so they continue to function in accordance with this Agreement despite the update or modification to the EHR.

If there is an update or other modification of third party software or services to which the EHR is interfaced, EHR Vendor shall work diligently with the third party that issued the update or modification to promptly revise the interface so it still functions in accordance with this Agreement.

In the event that Customer experiences any errors or other problems with an interface provided by a third party, EHR Vendor agrees to work cooperatively with both Customer and the third parties that provided the interface, and/or the software or services being interfaced to resolve such errors or other problems, including the sharing of the Software Documentation and any other information relating to the EHR system necessary to resolve such issues in a prompt and reliable manner.

Without limiting any other obligations of the EHR Vendor under this Agreement, if Customer elects to use additional third party software or

services in the future and proposes that the EHR Vendor will develop interfaces to such additional software or services, the EHR Vendor and Customer shall promptly negotiate in good faith to determine the reasonable cost and time required to develop interfaces to such additional software or services, with such costs not to exceed the documented time incurred by employees of the EHR Vendor at the then current hourly rates that would be charged by EHR Vendor for similar services provided under this Agreement.

EHR Vendor shall cooperate with the development of any interfaces between its EHR and any third party software or services provider identified by Customer during the term of this Agreement.

As used herein, "interfaces" includes, without limitation, any technical manner by which Customer's system receives or transmits data to another system.

You should also remember that interface development typically requires cooperation from both your EHR vendor and the developer of any software or services to be interfaced. It is therefore helpful to include contract language requiring cooperation on interface development in **all** of the information technology contracts you sign, not just your EHR contract.

Integration of an outgoing EHR vendor's technology with the EHR of a new incoming EHR vendor in order to transfer data is addressed in *Section 9 – Transition Issues: Switching EHRs*.

5.2 Integrating Third Party Products and Providing Access to Data

Making certain that your EHR contract does not unduly restrict your ability to integrate third party technologies and services may be important to your ability to leverage data to deliver better and more efficient care, or to take advantage of emerging technologies that make sense to you. As health care delivery is affected by increased cost and quality demands, health care provider organizations are increasingly looking to third-party vendors to provide innovative technologies and solutions that enhance the functionality of their health IT and enable them to improve their delivery and management of care. For example, a team of health care professionals working in multiple facilities with different EHRs may use a third-party application to help them collect and synthesize patient information from multiple sources, presenting population insights and quality and performance indicators in a single "dashboard" display.

Unless you negotiate more favorable terms, a standard form EHR contract may not allow you to give third party developers access to the EHR technology or to the data necessary to provide services that may fall outside of the scope of core EHR functionality such as the following:

- quality analysis and benchmarking functions across multiple providers (not limited to "internal operations");
- public health reporting;
- downloads of data to health information exchanges (HIEs);
- measuring population health and contributing to clinical data registries, often in the context of accountable care organizations (ACOs);
- the defense of a medical malpractice claim;
- clinical research trials;
- financial audits;
- data privacy and security forensic audits;
- receipt of clinical data from the patient's medical devices or from mobile and other apps used directly by a patient;
- providing clinical information to providers at the point of care (for example, via third party technology to assist a provider in interpreting genetic test results); and
- secure texting services enabling real-time communication with patients.

Having this flexibility is important because your EHR vendor may not offer certain types of products or services, and even if it does, you may determine that

another vendor has developed an innovative or better approach for your particular requirements. This is seen in the growing market for innovative "plug and play" technology that can enhance the functionality and value of your EHR.

To help assure that you can leverage new innovations and the most appropriate solutions for your needs, you should consider negotiating appropriate rights and obligations in your EHR contract, including the right to grant third-party developers and service providers sufficient access to your EHR and data to provide services for you.

(a) Variations Across EHR Vendors and Service Models

Certain EHR vendors may severely limit opportunities to customize or to make enhancements to your EHR. In other cases, a cloud-based EHR vendor may use its control over data hosted on its servers to act as a gatekeeper, charging significant fees for access to the data that, as against the vendor, you own. An EHR vendor may also attempt to impose restrictions or limitations on your ability to:

- exchange data with competing products or services;
- customize or enhance your EHR to integrate new sources of data; or
- leverage technologies developed by third-parties.

It is ultimately up to you to decide how much flexibility you will need to customize and enhance your EHR and to what extent you are willing to forego such flexibility in exchange for other potential benefits that may be offered by your EHR vendor. You should carefully assess your needs and should raise these issues early in your discussions with potential EHR vendors.

(b) Terms Affecting Your Ability to Integrate Data and Third-party Technologies

Integrating third-party technology with your EHR may require you to give your third-party developer access to portions of the EHR that your EHR vendor views as proprietary or confidential. This is understandably a very sensitive issue for EHR vendors, who place significant value on the intellectual property associated with their EHRs. (See *Section 6 – Intellectual Property* for a discussion of intellectual property issues arising in EHR contracts). Nevertheless, health care provider organizations increasingly view it as important to have the EHR vendor commit to granting third-party developers access to some information that may be proprietary or confidential, subject to appropriate non-disclosure and other agreements, so the provider can benefit from innovative technologies and services. This information may include, for example, the documentation and application programming interfaces (APIs) that are necessary to provide the third-party service.

Many standard form EHR contracts contain restrictions in this regard, starting with expansive definitions of intellectual property and confidential information. In some cases, an EHR vendor may refuse to allow third-party access to any of this information, or it may agree to do so only if the third party and/or its employees agree not to compete with the EHR vendor in a broad range of products and services, some of which may have no relationship to the vendor's intellectual property.

Health care provider organizations have reported difficulties negotiating reasonable exceptions to these types of restrictions, so it is advisable to raise this issue early in your negotiations if third party innovations are important to you. Assuming you value this flexibility, you should carefully evaluate whether an EHR vendor will provide reasonable access to its EHR technology when you are selecting your preferred EHR. You should also ensure that your EHR contract addresses any costs that an EHR vendor proposes to impose in connection with the testing of third party applications.

(c) Terms Limiting Access to Data or Data Formats

While EHR vendors may have a valid basis for strongly asserting their intellectual property rights to protect proprietary software, difficulties arise if an EHR vendor broadly claims intellectual property rights or trade secret protections to limit your ability to access and use data that you have contributed to the EHR

and that, as against the vendor, you own. Because most third party services rely on data stored in the EHR, problems arise if that data is not readily available or is not provided in a usable form.

Even when the data is available, a great mass of unstructured patient data is extremely difficult for a third party developer to use. Instead, the effective use of such data requires the third-party developer to have access to the data models and "data dictionaries" that the EHR vendor typically views as proprietary information. There have been instances of EHR vendors not being willing to make such information available on reasonable terms, which severely impairs the ability of health care provider organizations to have a reasonable choice of alternative technologies to improve patient care and efficiency. Some health care provider organizations feel that a lack of access to information about data models and similar information should not effectively force them to use only the EHR vendor's applications when there may be more innovative solutions available from third parties.

The EHR vendor may have reasonable concerns about whether the third party solution will corrupt patient data and whether it would be expected to support unknown third party technology, but ideally the parties can work together in good faith to negotiate reasonable terms of access. For example, if the EHR vendor requires a third-party developer to sign a confidentiality agreement regarding the EHR's data dictionary, the agreement should not also impose a non-compete obligation on the third-party developer that severely limits its ability to perform a wide range of technology services that do not utilize the data dictionary. In addition, if the terms of access impose a fee on you or the third-party developer, you should try to negotiate a reasonable fee upfront. The amount of effort may be unknown in advance, so you could base the fee on the time that the EHR vendor actually spends providing the necessary information and access, multiplied by the rate that applies for comparable services under the EHR contract.

One approach to managing the challenge of having your EHR vendor deal with third party developers would be to have the EHR contract address the following matters to the extent relevant to your needs (there may of course be other points that you will also need to negotiate depending on the specific technology and your goals):

- the EHR vendor will work in a timely and good faith manner with third parties who need access to the data and EHR technology in order to develop and implement additional services for you. You and the third party developer would also make the same commitment;
- data in the EHR will be provided to you or the third-party developer without charge to the extent that you or the third party developer reasonably requests it for the development and/or ongoing use of the third party technology;
- to the extent necessary and subject to a reasonable confidentiality agreement and possibly a reasonable non-compete agreement (which should be no broader than necessary, as discussed above), the EHR vendor will: (i) provide access to the EHR data using a transfer mechanism that facilitates ease of use, which might comprise, as necessary, access to a copy of the backend database that holds the EHR data (sometimes referred to as a replicated data store feed), a data warehouse feed, and/or an API; and (ii) make information available to the third party developer that will enable the third party developer to use relevant EHR data in the developer's technology in an efficient and interoperable manner (such as a data dictionary or glossary, the database structure and data models);
- if the EHR vendor requires a fee for access to such information, it should be reasonable (perhaps based on the time actually expended in providing the information and access to the data at the rate then in effect for similar services); and
- your use of the third party's technology should not cancel any warranty of the EHR vendor unless such use in fact harms the data or the EHR technology itself.

6. INTELLECTUAL PROPERTY ISSUES

Your contract with an EHR vendor will give you the right to use certain software, documentation, services, and possibly other intellectual property (IP). Your rights to use this IP (and to allow others to do so on your behalf) will be limited to the conditions specified in your EHR contract. The IP provisions are important in several respects, including their role in protecting you from the claims of third parties alleging IP infringement and governing whether and to what extent you are allowed to customize or enhance your EHR (for example, adding functionality or integrating other sources of data that are useful to your health care professionals and operations). They will also affect whether you are allowed to share or commercialize any enhancements that you may make. For these and other reasons discussed below, it is important that you review and understand how the IP clauses in your contract work.

6.1 Intellectual Property Rights: What Are They and Why Should You Care?

Many aspects of your EHR—including software, documentation, databases, processes, and even the layout and presentation of certain information to users—may contain IP that belongs to your vendor and is protected by law. The extent of such protection will depend on the type of IP, whether a patent has been obtained, whether there are agreements to hold the IP in confidence, and other factors. There will also be parts of your EHR that are not your vendor's intellectual property, such as the health information you obtain from or about your patients and record in your EHR, and other facts about your business such as fee schedules, professional credentials, and quality scores. A full description of each type of IP right is beyond the scope of this guide, but the following may provide a useful introduction:

A **copyright** typically protects only the "form of expression" of an original work of authorship, not the underlying ideas or information. The EHR vendor's software, documentation, images, and databases are usually protected by copyright. Copyright protection exists automatically from the moment an original work is created and does not require registration with the federal Copyright Office (although registration does confer some additional protection for the copyright owner).

A **registered patent** gives the patent holder the right to prevent others from using, making, selling, or importing the "invention" covered by the patent. Patents can only be obtained by applying and receiving a patent from the U.S. Patent and Trademark Office. Once obtained, patents may be enforced even against others who have independently developed the same invention. When a patent is granted, the invention is disclosed to the public so it would no longer be confidential information. A machine or a process may be patented if it meets specific criteria and the extensive filing and review process has been successfully completed. It is possible that a process used by an EHR could receive patent protection if the statutory requirements were met and the necessary time and expense were incurred to obtain a patent.

A **trade secret** refers to certain confidential and commercially valuable information such as techniques and processes. Trade secret law protects the information itself, not just the "form of expression" protected under copyright law. The details vary by state and under federal law, but typically trade secret protection is available only for information that: (i) provides a benefit by not being known to competitors; (ii) is kept confidential within the EHR vendor's organization; and (iii) is subject to confidentiality agreements if it must be disclosed to third parties. EHR vendors often seek to protect their trade secrets through confidentiality or non-disclosure agreements with customers and other third parties.

If the EHR is provided for operation on your own equipment or on hosted equipment that you have arranged, you should receive a license from the EHR vendor to use all software, documentation and other IP that may be included in the EHR. The EHR contract may also attach separate licenses for you and third parties to sign so that you can use third party products. The EHR vendor is typically not a party to

these third party licenses. You need to review and possibly negotiate these third party licenses with respect to IP and other rights, although you may not have much negotiating leverage if they are licenses for commercial off-the-shelf software.

By contrast, the EHR contract for a cloud-based EHR may grant you the right to use the EHR services without expressly granting you a license to the software or other IP because you may not need a license to use the services. Nevertheless, there may be benefits to obtaining a license under a cloud-based EHR contract, including the ability to continue to use the EHR software in the event of a cloud-based vendor's bankruptcy. This is a complex area so you should seek legal advice regarding the possible benefits of a license under a cloud-based EHR contract.

To protect their IP, many EHR vendors limit the scope of the license they will grant to users of their EHRs. In addition, standard form EHR contracts often include very broad non-disclosure obligations and other restrictions that will apply to you unless you negotiate these provisions. See *Section 2 – EHR Safety and Security: A Shared Responsibility* for a discussion of exceptions to an EHR vendor's non-disclosure agreement that may be necessary to permit providers to disclose issues involving patient safety that arise in connection with EHRs. Also see *Section 5 – Fostering Interoperability and Integration* for a discussion of how standard form EHR contracts may restrict a health care provider organization's right to allow third parties to access data dictionaries and other information necessary to effectively use patient data from the EHR to improve patient care and to implement alternative payment models.

You need to ensure that your EHR contract provides you with sufficient rights to use all of the vendor's IP that is necessary to support:

- your legal obligations under HIPAA to give your patients (and their designees) a copy of the patient's protected health information on request, including by direct transmission from your EHR; and
- your implementation of impending Meaningful Use and other federal or state requirements that will require that you facilitate access to, and the exchange of, a patient's information, including with patients and persons they authorize; and using a variety of technologies, including consumer-facing applications.

As discussed in *Section 5 – Fostering Interoperability and Integration*, you may also wish to ensure that your EHR contract provides you with rights to use and, subject to appropriate safeguards, disclose to third parties the vendor's IP for the purpose of integrating third party technologies and services that are important to you.

6.2 Ownership of IP Developed Under an EHR Contract

Some health care provider organizations make a significant investment in the customization of their EHR, including the development of interfaces for certain specialties. Sometimes this work is done by the health care provider organization's EHR vendor, but often the work is done by the health care provider organization's in-house IT and informatics teams. You may find that your ideas or efforts have resulted in a significant improvement to the way your health care professionals use your EHR or interact with patient data, and you may wish to share or commercialize those improvements. You may also have paid your EHR vendor to develop customizations or an enhancement that it later markets to many other customers for additional fees. Although you may feel entitled to some compensation in these situations, you would not be entitled to any payment or credit for your contributions under many standard form EHR contracts, unless you negotiate that right.

The lack of compensation in these situations is due to language in many standard form EHR contracts that grants the EHR vendor exclusive ownership of all modifications, developments, customizations, derivative works, inventions, ideas, enhancements, or other improvements (collectively, "Improvements") in or related to the EHR vendor's IP. This language may apply even if the Improvements were developed only through your efforts and did not involve the use of any of the EHR vendor's IP. The contract or statement of work for customizations or enhancements may also grant the EHR vendor ownership rights in these Improvements even if you have agreed to pay the

EHR vendor a significant amount for developing them. Typically you would receive only a license to use the Improvements while you were using the base EHR software or services and the Improvements would be subject to the same restrictions on disclosure and use as the base EHR software and services.

At a minimum, you should understand the impact of these ownership provisions and the fact that many EHR vendors would resist changing them. For example, you might attempt to negotiate a lower price for the enhancements or customizations you are paying for because, if the standard language is not revised, the EHR vendor may be able to charge other customers for the development you have funded. If you would like to receive a financial benefit from the Improvements that you have created or funded by licensing them to others, typically you will need to negotiate to have sole or joint ownership of the Improvements. You might also be able to negotiate to have the EHR vendor pay you a royalty on its further use of these Improvements. You should address these issues early in your negotiation of the EHR contract and, if applicable, the statement of work for the customization or other enhancement.

6.3 IP Claims of Third Parties

If your EHR vendor does not have all of the rights necessary to provide the software or service without "infringing" or violating the IP rights of others, you could be sued. Under IP law, a third party that holds a patent or copyright can sue anyone who uses software or services that "infringe" or violate the third party's exclusive right to use the patent or copyright. IP law also protects trade secrets from being taken or used without permission. This means that you could be sued by a holder of an infringed patent or copyright or a misappropriated trade secret even though you are only a licensee of the EHR software or the user of services in a cloud-based EHR.

It is common for the holder of a patent with infringement claims against an EHR vendor to approach the vendor's customers with a demand to "cease and desist" using the allegedly infringing technology. Having to suddenly stop using the EHR in this situation could seriously impact patient care and your business. The patent holder may also claim monetary damages from the vendor's customers that use the allegedly infringing technology. As a result of this pressure, some customers enter into a license and pay the patent holder a royalty in order to settle the claims. However, this should not be necessary if the EHR vendor has agreed to defend and indemnify you for third party IP claims.

Because the EHR vendor is typically in the best position to make sure that its software or service does not infringe any third party's IP, your EHR contract should include a non-infringement warranty as discussed in *Section 3 – System Performance: Ensuring Your EHR Meets Your Expectations*, as well as a promise from your EHR vendor to "defend and indemnify" you from patent and copyright infringement. It would also be best practice to seek an indemnity for claims that a third party's trade secrets have been misappropriated or used without permission. The EHR vendor, if it gives an intellectual property indemnification, often asks to receive prompt notice of the claim, to be able to control the defense and settlement of the claim, and to receive cooperation from you as the indemnified party.

Some EHR vendors try to limit their possible liability for IP infringement by allowing the EHR vendor to replace or modify the software or service or even terminate the license or service arrangement if an infringement claim cannot be settled on terms acceptable to the EHR vendor. You should carefully review the indemnification provisions with respect to this issue and the others described below:

- if the EHR vendor can replace or modify the software or service, does it promise that the new or modified version will still have all of the features and functions of the original?
- if the software is replaced or modified, will the EHR vendor pay for necessary retraining of your personnel and modification of any interfaces that must also be changed?
- if the EHR vendor terminates the license or service, what portion of your fees and other expenses will be refunded?
- how will the transition to new software or services be handled if the EHR vendor no longer has the necessary IP rights? and

- does the language exclude responsibility for IP infringement claims based on a combined use of the EHR vendor's technology with technology that it did not provide? You may want to consider modifying such exclusions if the EHR vendor's product requires or relies on the use of other technology.

You may also be asked to warrant that you have all rights necessary to post or upload information to your cloud-based EHR and to indemnify the EHR vendor if a third party claims that data you post or upload violates the third party's IP rights. This may be reasonable, but you should make certain you understand the implications of this language before signing your EHR contract. For example, you need to make sure that you own or have the necessary right, such as an assignment or copyright license, to post or upload anything that you or your employees did not create.

7. MANAGING RISKS AND LIABILITY

EHRs can reduce medical errors, improve patient safety, and support better patient outcomes. There are certain business and financial risks inherent in the implementation and use of your EHR, however, which need to be carefully considered while negotiating a contract with an EHR vendor. Accordingly, you need to ensure that you understand how your EHR contract addresses and apportions risk and liability between the parties.

Consider, for example, the situation where your EHR software has been programmed to translate narrative diagnoses for outpatient physician visits into ICD-10 codes. You notice and alert your EHR vendor to errors in the crosswalk, including the incorrect mapping of a narrative diagnosis of diabetes to a code representing a diagnosis of diabetes associated with ESRD. Your EHR vendor responds to the error by implementing software corrections as part of non-urgent periodic updates and does not correct any previously misreported diagnoses. The effect of such a software error on your business could be significant, especially if your EHR contract does not provide protections against your exposure to such risks and associated liability. If your medical record entries are populated with incorrect patient diagnoses, your patients are at risk of associated treatment errors, and you are at risk of potential medical malpractice liability as well as exposure for false claims liability if governmental insurers were billed using incorrect diagnoses codes. If your EHR vendor's liability under your EHR contract is limited by the exclusion of certain types of damages and by a low liability cap (as is the case in many standard form EHR contracts), you may be able to recover only a fraction of the amount of financial damage suffered by you, despite the cause of the damage being the EHR vendor's defective software and inadequate support.

7.1 Evaluating Your Risks

A first step in understanding and managing your risks is to undertake a thorough risk assessment. A risk assessment typically includes the following steps: (i) identifying risks associated with the implementation and use of your EHR; (ii) estimating the likelihood and magnitude of the identified risks; and (iii) determining whether the projected impact of those risks exceeds your risk tolerance. The results of your risk assessment will inform you about the issues to be addressed in your EHR contract to minimize your exposure to risk and associated liability. It will also educate you about other risk reduction strategies you should explore, such as consulting with your insurance carrier. Your risk assessment may benefit from a review by an attorney experienced in negotiating EHR contracts.

7.2 Allocating Risk and Liability

The parties to an EHR contract can agree on how liability for risks arising under the EHR contract will be allocated. It is highly recommended that EHR contracts be structured to allocate responsibility for risk to whichever party has the most control over the factors giving rise to a particular risk and is best positioned to prevent and mitigate such risk.

One approach is to use "risk transfer" provisions in your EHR contract that explicitly allocate specific risks and liabilities, making either you or your EHR vendor solely responsible for any loss or damage arising from each specified risk or liability event. This can be accomplished through a combination of indemnification and hold harmless provisions,

limitation of liability clauses, and insurance coverage requirements for specified risks of loss. These risk transfer provisions—and what you should know about them—are discussed in more detail in the subsections that follow.

Many standard form EHR contracts contain risk transfer provisions. Because these contracts are drafted by the EHR vendor's lawyers, they typically assign most risks and liabilities to the customer. This may be true even for risks arising from the vendor's acts or omissions that are beyond your ability to prevent or control. To achieve a more appropriate and balanced allocation of risks between you and your EHR vendor, it will often be necessary to negotiate these risk transfer provisions. An alternative to negotiating specific risk sharing provisions is to agree that each party to the contract will take responsibility for its own actions and will be liable for any losses occasioned by its own acts or omissions. This is consistent with the position that a court would generally adopt by allocating liability between you and your EHR vendor if your EHR contract were silent on the issue of risk and liability.

7.3 Indemnity Provisions

One of the most common methods of allocating risks and liability in EHR contracts is through the use of indemnity provisions, through which one party to the contract (the "indemnifying party") typically agrees to indemnify and to hold harmless the other party for certain types of claims and under certain circumstances. The indemnifying party agrees to reimburse or "make whole" the other party with respect to certain types of claims by paying all costs (including attorney's fees), claims, judgments, awards, penalties and amounts agreed to in full settlement of the claim. The indemnifying party also may agree to "defend" the other party, meaning that it must hire counsel to defend the claim on behalf of the other party in court. A vendor's standard form EHR contract may contain several different types of indemnity provisions, as further described below.

(a) Indemnifying Your EHR Vendor

Most standard form EHR contracts will contain a provision under which the EHR vendor requires the provider to indemnify the vendor for certain risks and liabilities. It is important that you carefully consider and understand the scope of any indemnity that you will provide to your EHR vendor. Common types of indemnities cover the following:

- **General Indemnity**: Some standard form EHR contracts will ask you to provide a general indemnity in favor of the EHR vendor. This type of provision is often drafted broadly and may hold you responsible for losses suffered by the EHR vendor even in the absence of any negligent or intentional act on your behalf. Depending on the breadth of the indemnity language used, as well as any related liability provisions relating to the types and total amount of damages, the effect of this type of provision may be that your EHR vendor is excused from all liability to you under the contract, including, for example, liability associated with poor performance, interruption of service, defective software, and breach of privacy or security.
- **Third Party Claims**: EHR vendors will often ask health care provider organizations to agree to indemnify and defend the EHR vendor against claims brought against the EHR vendor by third parties (organizations and individuals who are not parties to the EHR contract). The types of third party claims for which EHR vendors typically attempt to make their customers liable include: (i) personal injury (including death); (ii) damage to the third party's property; and (iii) claims related to injuries of the EHR vendor's personnel (i.e., workers' compensation claims), agents or subcontractors.
- **Patient Claims**: Another type of third party claim involves claims asserted by patients of the health care provider organization with respect to injury that was caused to some extent by an error in the EHR vendor's EHR software or related services. Many standard EHR contracts contain a provision requiring a health care provider organization to indemnify the EHR vendor for patient claims arising from EHR errors, even if the harm was caused by the EHR software or service, in whole or in part.

In general, you should be reluctant to agree to these types of indemnity provisions because they run

counter to the basic legal principle that each party is responsible for its own acts and omissions. Accordingly, contractual risks and related liabilities should be allocated to whichever party has the most control over the factors giving rise to a particular risk.

When faced with these provisions, you should negotiate with your EHR vendor to attempt to strike a more appropriate and balanced allocation of risks and liabilities. As an illustration, instead of agreeing to a "Patient Claims" indemnity being included in your EHR contract, you may suggest a more balanced provision that makes each party responsible for its own negligent acts and omissions (sometimes referred to as "comparative negligence" or "contributory negligence") or intentional misconduct (see discussion below). Your EHR vendor may object to a more balanced allocation of liability by arguing that it is too difficult to determine how various factors in patient care resulted in a poor outcome for the patient and therefore it is you who should be solely responsible. A counter argument is that your responsibility is limited to diagnosing disease, prescribing treatment, and performing related tasks that constitute the practice of medicine. For example, to the extent that the EHR vendor controls whether the software accurately records patient data entered by you and transfers it as directed by you, and assuming that you act in accordance with the EHR's instructions, then your EHR vendor should be responsible for patient harm that arises from the EHR's failure to accurately retain or transfer such data.

Another potential response to an EHR vendor's attempt to impose broad, vendor-favorable indemnity provisions is to request that any indemnity provision operate on a mutual basis, making each party liable for the consequences of their own acts and omissions. An example of mutual indemnification in which each party is responsible for its own negligent acts or omissions or intentional misconduct is set forth below. This approach may be more acceptable to you, but it should not be used without legal advice about your particular situation and applicable state law.

Example Contract Term 16

Each party (the "Indemnifying Party") agrees to defend, indemnify, and hold harmless the other party and its servants or employees (the "Indemnitee") against any claims, costs, liabilities, and expense arising from or attributable to the Indemnifying Party's negligent acts or omissions and intentional misconduct which is brought against an Indemnitee in connection with the EHR system or related services or the Indemnifying Party's breach of its responsibilities under this Agreement.

If your preferred EHR vendor is unwilling to agree to a balanced indemnity or to mutual indemnification, then you could consider an alternate position that the EHR contract remain silent on the parties' liabilities. In the absence of any contractual provision to the contrary, most courts would allocate responsibility using a balanced approach consistent with common law that assigns liability to the party or parties that caused or contributed to the loss. As always, it is strongly recommended that you obtain the advice of experienced legal counsel on these issues.

(b) Indemnifying Your EHR Vendor: HIPAA Claims

Some EHR vendors reportedly are asking their customers to indemnify them for damages associated with the EHR vendor's obligations as "business associates" under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or under state privacy protection laws. You should seriously consider objecting to assuming liability for an EHR vendor's breach of its obligation to safeguard the privacy or security of information in the EHR because this is not a risk that you can necessarily control. Additionally, the HITECH Act requires that business associates directly comply with the HIPAA Security Rule and HIPAA's business associate safeguards, including: (i) limiting use and disclosure of protected health information (PHI) as specified in the Business Associate Agreement or as required by law; (ii) facilitating access, amendment and accounting of disclosures; (iii) opening books and records to the Department of Health and Human Services; and (iv) returning or destroying PHI upon contract termination.

(c) EHR Vendor's Indemnification of You: Intellectual Property Infringement

An EHR vendor should agree to indemnify and defend you against a third party claim brought against you alleging that the EHR vendor's EHR software and/or services infringe the third party's patent, copyright, or other intellectual property rights. This is because responsibility for the software falls squarely within the responsibility and control of the vendor. If it is not already covered in your draft EHR contract, then you should seek to have this obligation broadened to also cover misappropriation of trade secrets.

However, you should be aware that EHR vendors may try to limit their liability for intellectual infringement by including language that gives the vendor the option to cancel the EHR contract in the event that an intellectual property infringement claim is made and, for an EHR contract based on licensed software, refund only a portion of the license fees.

In these circumstances, you should analyze whether the EHR vendor's rationale that its right to terminate and provide only a limited refund is an appropriate allocation of this risk. For example, if the EHR vendor's contract stated that it may elect to terminate the contract and refund a portion of the license fee initially paid by you based on a useful life of three years, and the infringement occurred after two years, then the EHR vendor could terminate and refund only one-third of the license fee. You instead may argue that a longer useful life would be appropriate and that the amounts to be refunded should include implementation and training fees as well reasonable costs of a replacement EHR.

Please see *Section 6 – Intellectual Property Issues* for a further discussion of this topic.

(d) Indemnification for Costs

Another important aspect of indemnification provisions is the description of the costs and expenses from which the indemnified party will be held harmless. Ideally, the indemnity should extend to all claims, demands, liabilities, obligations, settlements, awards, costs, penalties and expenses (including attorneys' fees and court costs) incurred by the indemnified party as a result of the indemnifying party's conduct or third-party claim. In an effort to limit their indemnification obligation, some EHR vendors may seek to limit the costs and expenses they are required to pay to only those that are "finally awarded" to the indemnified party. This language excludes coverage of amounts agreed to in settlement and all costs incurred by the indemnified party in its own defense. You therefore may wish to make an informed judgment with respect to language limiting the costs that are recoverable to you. In the event that you are the indemnifying party, however, then it may be to your advantage to limit such costs.

(e) Related Obligations

Indemnity provisions typically also include the following obligations on behalf of the party seeking to be indemnified: (i) promptly notifying the indemnifying party of any third-party claim; (ii) giving the indemnifying party sole control over the defense of the claim; and (iii) providing the indemnifying party, at the indemnifying party's expense, all cooperation reasonably necessary to assist in the defense. These obligations are often stated so that they are conditions to the right to be indemnified; in other words, the indemnifying party will have no obligation to indemnify unless these obligations are fulfilled. A compromise to this EHR vendor-oriented position is to provide that the obligation to indemnify will be relieved only to the extent that the EHR vendor's ability to indemnify is hindered by the failure of the party seeking indemnification to perform these obligations. This may be especially important with respect to the obligation to provide prompt notice of the claim.

(f) Third Party Beneficiaries

The EHR vendor contract should state that there are no third party beneficiaries, so that third-party claimants will not be able to benefit from contract provisions intended to assist the EHR vendor or you.

Example Contract Term 17

This Agreement is made solely for the benefit of the Customer and the EHR Vendor and their respective successors and assigns. No other person or entity shall have any right, benefit, or interest under or because of this Agreement, except as otherwise specifically provided herein.

7.4 Limitations of Liability

Limitations of liability are standard components of commercial contracts. In standard form EHR contracts, they are typically drafted with a view towards limiting the vendor's financial risk for claims that may arise from problems with the EHR. As illustrated by the introductory example, limitations of liability can have a significant effect on your ability to recover damages from your EHR vendor in the event of problems with your EHR. The financial consequences of such problems may not be covered by your insurance coverage and may have a significant budgetary impact.

Limitation of liability provisions typically include two components:

- limits as to the ***total dollar amount*** of damages for which the EHR vendor could be liable under the agreement (sometimes referred to as a "cap"); and
- limits as to the ***types of damages*** (i.e., consequential, special, incidental, punitive) for which the EHR vendor seeks to disclaim liability.

The following is an example of limitation of liability provisions drafted from the EHR vendor's perspective—in other words, ***not favorable to the health care provider organization and should not be used***:

> **LIMITATION OF LIABILITY**. UNDER NO CIRCUMSTANCES SHALL EHR VENDOR BE LIABLE FOR ANY REASON FOR ANY AMOUNT IN EXCESS OF THE TOTAL AMOUNT PAID DURING THE PRECEDING TWELVE (12) MONTHS WITH RESPECT TO THE ITEM OF SOFTWARE OR THE SERVICE TO WHICH SUCH LIABILITY RELATES REGARDLESS OF WHETHER SUCH CLAIM ARISES IN CONTRACT, TORT, OR OTHERWISE.
>
> **EXCLUSION OF CONSEQUENTIAL DAMAGES**. UNDER NO CIRCUMSTANCES WILL EHR VENDOR BE LIABLE FOR ANY INCIDENTAL, SPECIAL, EXEMPLARY, CONSEQUENTIAL OR OTHER INDIRECT DAMAGES ARISING UNDER OR RELATING TO THIS AGREEMENT OR TO ANY SERVICES, SOFTWARE, OR OTHER MATERIALS PROVIDED BY EHR VENDOR TO CUSTOMER, INCLUDING, WITHOUT LIMITATION, LOST DATA, LOST PROFITS, OR THE FAILURE TO ACHIEVE ANTICIPATED SAVINGS, WHETHER OR NOT SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY HEREIN.

In the examples above, the first provision (titled "LIMITATION OF LIABILITY") is an example of a limit on the ***total dollar amount*** of damages for which the EHR vendor could be at risk regardless of the type or amount of damage suffered by the customer. The amount should be carefully evaluated by you because it limits how much you may be able to recover from the EHR vendor if the EHR does not work or other problems arise. Dollar amount limitations are often stated as "total," "cumulative" or "aggregate." This means that all damages to which the injured party is entitled under the agreement, throughout its term, are accumulated. Once the limit is reached, the injured party no longer has the right to recover any more damages. This type of limit may be inadequate to protect your interests. The dollar amount limitation should be based upon the true maximum amount of damages to you that could result from a breach by the EHR vendor.

The second provision in the example above (titled "EXCLUSION OF CONSEQUENTIAL DAMAGES") is an example of a limit on the ***types of damages*** that the EHR vendor would be responsible for. This type of provision should be carefully reviewed, preferably in conjunction with an attorney experienced in the negotiation of EHR contracts. The following information is provided only as background for that discussion:

- "**Direct**" damages are not typically excluded from an EHR contract and may be recovered.

However, some EHR vendors may seek to limit your recovery of direct damages by placing a cap on the amount of recovery or excluding certain types of direct damages. A claim for direct damages would involve assessing what costs you incurred ***as a direct result*** of the EHR vendor's breach—for example, did you need to obtain additional software or equipment? You should carefully review any contract language that seeks to limit either the amount or type of direct damages that are recoverable under your EHR vendor contract. While most EHR vendors will not agree to unlimited liability for direct damages, you should have a sufficient understanding of the potential for direct damages to negotiate a damages cap that provides reasonable protection.

- "**Consequential**" damages are those that are not a direct result of an act, but rather a consequence of the initial act such as lost profits, damage to reputation (i.e., goodwill), or other types of harm that are foreseeable and directly traceable to the breach of contract. As in the example above, consequential damages often are excluded by EHR vendors in standard form EHR contracts.
- "**Lost data**" may not fall into the definition of 'consequential damage' so EHR vendors often try to specifically exclude this type of damage in an effort to transfer the risk of lost data to you. A loss of data often is very serious to a customer and reducing the risk of data loss may, for example, have been an important reason that an EHR vendor's cloud-based EHR service was selected. Attorneys for health care provider organizations usually object to excluding damages for lost data unless the health care provider organization has agreed to accept full responsibility for data backup. In addition to addressing legal liability for lost data, you need to understand what action to take in advance of a privacy or security breach to reduce the risk that lost data will adversely affect continuing patient care. For a more complete discussion of data control issues, please see *Section 4 – Data Rights: Managing and Safeguarding EHR Data*.

7.5 Negotiating Limitation of Liability Provisions

Where an EHR is provided as a service (e.g., via a cloud platform), the EHR vendor will often try to limit its total liability under the EHR contract to the amount of the fees (or multiples thereof) received during a specific period of time (the example above used 12 months). If the EHR is provided as a licensed software solution, then the amount of the license fee may be used as the reference point for the liability cap. You should consider very carefully whether it is in your best interests to accept a limitation of liability provision that is formulated by reference to the amount paid for a service or license. This is because the proposed cap has no relation to the potential damages that you may incur as a result of the EHR vendor's negligence or intentional misconduct. You should, as part of any risk assessment (discussed in subsection 7.1 above), determine the likely amount of damages that may flow from a breach of contract by the vendor or from the vendor's negligence or intentional misconduct, and use this as a starting point for determining the quantum of any liability cap. A security failure, for instance, may be a breach of your EHR contract depending on the particular circumstances, and could cause you to incur significant costs and financial loss. If you were to accept an artificially low cap, and incurred a liability which exceeded that cap, the resultant loss likely would not be covered by your insurance carriers since the loss is an assumed contractual liability (discussed in further detail below).

EHR vendors may state that, without limitations of liability, the prices that EHR vendors would charge to cover their risk would make their product and/or service much more expensive. If you have been advised by the EHR vendor that the limitation on liability is "priced into" the agreement, then you may wish to ask the EHR vendor what the contract price would be if the limitation of liability is stricken from the agreement. In short, you should not be asked to be in the position of subsidizing a vendor's negligence or tortious conduct.

Another means of managing the exposure created by agreeing to a limitation of liability provision is to negotiate for the exclusion of certain types of claims,

whether financial or by type of damage. Examples of the types of damages that you should consider excluding from a limitation of liability include the following:

- claims subject to indemnification (e.g., intellectual property indemnification);
- personal injury (including death) and property damage;
- breach of confidentiality and breaches of a EHR vendor's business associate obligations under the HIPAA Rules and HITECH;
- damages arising from the other party's negligence or willful misconduct; and
- damages related to the EHR vendor's repudiation of or wrongful refusal to perform its obligations under the contract.

The reason that these types of claims or damages should be considered for exclusion is because the nature of the harm is such that the injured party would not be adequately compensated if the right to recover monetary damages were limited. For example:

- if the negligence of the EHR vendor's personnel caused a fire at your office that made it unusable for patient care, then you may wish to seek damages from the EHR vendor for lost revenue without this being excluded as a type of consequential damages;
- if the EHR vendor were responsible for a disclosure of PHI in violation of the HIPAA Privacy or Security Rules, then the damages could include claims by federal and state governments and resulting penalties, the cost of mailing notices to patients whose PHI was affected and claims by patients for resulting identity theft or damage to reputation under state law, some of which may otherwise be excluded as consequential damages; or
- if the EHR vendor refused to support the EHR or failed to return patient data to you as required, then you may wish to seek damages in excess of the financial limitation on direct damages because of the serious impact on your business operations and continuity of patient care.

An example of a limitation of liability term that may more reasonably limit the scope of the limitation of liability provided to the EHR vendor is as follows:

Example Contract Term 18

LIMITATION OF LIABILITY. IN NO EVENT SHALL EHR VENDOR BE LIABLE TO CUSTOMER ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT FOR ANY INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOST PROFITS OR LOSS OF GOODWILL, WHETHER BASED ON BREACH OF CONTRACT, WARRANTY, TORT, PRODUCT LIABILITY, OR OTHERWISE, AND WHETHER OR NOT EHR VENDOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. CUSTOMER AGREES THAT EHR VENDOR'S TOTAL CUMULATIVE LIABILITY FOR DAMAGES, IF ANY, SHALL NOT EXCEED THE AMOUNT OF $___ MILLION PER OCCURRENCE AND $___ MILLION IN THE AGGREGATE. NOTWITHSTANDING THE FOREGOING, THE LIMITATIONS ON LIABILITY SO DESCRIBED SHALL NOT APPLY TO DIRECT DAMAGES INCURRED BY CUSTOMER THAT ARISE IN CONNECTION WITH THE FOLLOWING: (i) CLAIMS FOR BODILY INJURY (INCLUDING DEATH); (ii) CLAIMS FOR DAMAGE TO REAL OR TANGIBLE PERSONAL PROPERTY SUSTAINED AS A RESULT OF EHR VENDOR'S PERFORMANCE OF ITS OBLIGATIONS HEREUNDER; (iii) CLAIMS, FINES AND INCURRED COSTS RELATING TO EHR VENDOR'S BREACH OF ITS OBLIGATIONS OF CONFIDENTIALITY HEREUNDER AND OF ITS OBLIGATIONS STATED IN THE BUSINESS ASSOCIATE AGREEMENT; (iv) CLAIMS FOR DOCUMENTATION OF PATIENT SERVICES FOR BILLING PURPOSES IN THE EVENT OF SYSTEM DOWNTIME; OR (v) ANY FINES, FEES OR ASSESSMENTS IMPOSED ON CUSTOMER BY A GOVERNMENTAL AUTHORITY AS A RESULT OF EHR VENDOR'S ACTIONS OR INACTIONS.

While this example has been prepared to provide only the vendor with the protection of a limitation of liability (and recognizes, through exceptions to that limitation of liability, legitimate damages for which the vendor should be responsible without limitation), you may reasonably negotiate to make the limitations

of liability provision mutual so that you will have similar protection to limited liability for certain types of claims and related damages.

While it always is prudent to minimize your exposure to risk and related liability by avoiding a limitation of liability provision in your EHR contract, this might not be practicable. If you must accept a limitation or a waiver of certain kinds of damages, then the contract should make explicit that there has been no waiver of direct damages caused by any acts or omissions of the EHR vendor. For example:

> **Example Contract Term 19**
>
> *Notwithstanding the foregoing waivers of damages and limitations of liability, in no event does Customer waive its right to seek recovery for its direct damages alleged to be caused by the EHR Vendor.*

Additionally, language exempting damages arising from data breaches and data loss should be in place in the event a cap is agreed to:

> **Example Contract Term 20**
>
> *Damages arising from data breach, data loss, or other breach of data privacy and security or failure of the EHR Vendor to comply with the confidentiality and data security obligations stated in this Agreement, or any Business Associate Agreement are not subject to the foregoing limitation of liability.*

7.6 Insurance Considerations

In reviewing indemnity and limitation of liability provisions, you should consider the effect that such provisions may have on your insurance coverage. It is also important to consult with your insurance carrier regarding the potential impact of indemnification on your insurance coverage. Under many insurance policies, if you agree to indemnify an EHR vendor for certain acts or accept liability that otherwise would be the EHR vendor's responsibility under applicable state law, then your insurance carrier may deny coverage for this "assumed" contractual liability.

For example, many EHR contracts state that the EHR vendor will be responsible only for acts of "gross negligence" as opposed to "negligence." Since the case law of most states permits recovery on the basis of "negligence," an insurance carrier may deny coverage on the basis that the gross negligence standard **excludes** acts of negligence and thus represents assumed liability on your behalf. In addition, most professional and general liability insurance policies exclude coverage for "assumed" contractual liability, which may operate to exclude liability assumed through indemnification language found in some EHR vendor contracts. You thus should check with your insurance carrier prior to agreeing to any such indemnity and limitation of liability provisions in EHR vendor contracts since you may not be insured for this business risk and any related damages would be your responsibility. Some insurance carriers may be willing to sell additional coverage for this situation, but both the scope of coverage and the cost would need to be determined.

Additionally, you may wish to require that the EHR contract require the EHR vendor to carry certain types and minimum levels of commercial general liability insurance as well as worker's compensation insurance as a means to ensure that financial resources will be available should a loss event occur in order to fulfill the EHR vendor's indemnification obligation. If the EHR vendor will have access to your IT infrastructure or holds your EHR data, then you also should require the EHR vendor to maintain cyber risk insurance. Given that both cyber-attack vectors and technologies are continually evolving, you should consider consulting with an experienced insurance broker to understand the full scope of the exposures and what controls may need to be implemented and reflected in your EHR contract.

The requirement to maintain certain types of insurance coverage also should extend to all subcontractors who indirectly provide goods or services through the EHR vendor, particularly if subcontractors will be providing goods or services onsite at your facility. You should request a Certificate of Insurance evidencing the types of insurance coverage with the amounts of coverage from the EHR vendor. Requiring EHR vendors to prove they carry sufficient insurance to cover the exposures inherent

in their services provides assurance that the EHR vendor has the financial capacity to cover a loss event. You may wish to ask whether you can be named as an additional insured on the EHR vendor's insurance policy. An example of a suitable insurance provision for an EHR contract is as follows:

Example Contract Term 21

Insurance. EHR Vendor shall maintain or cause to be maintained worker's compensation insurance in the amount required pursuant to state law, and commercial general liability insurance and cyber risk insurance for its agents, servants, and employees rendering services pursuant to this Agreement in the minimum amount of $___ Million per occurrence and $___ Million annual aggregate. EHR Vendor further agrees to maintain such insurance with the above stated coverage limits during the term of this Agreement and shall provide the other party with a Certificate of Insurance evidencing such coverage upon request. EHR Vendor also shall provide Customer with not less than thirty (30) days written notice prior to the cancellation or expiration of any insurance policy required to be maintained pursuant to this Agreement.

There is no one-size-fits-all insurance requirement. The types and amounts of insurance coverage should be customized relevant to a specific agreement. You should consider the activities the EHR vendor will perform in delivering the contracted goods and/or services as well as the risks arising from those activities as well as consult with your insurance carrier.

8. DISPUTE RESOLUTION: RESOLVING DISAGREEMENTS WITH YOUR EHR VENDOR

If a dispute were to arise between you and your EHR vendor, your ability to navigate and resolve that dispute in a timely and cost-effective manner will be assisted greatly if your EHR contract lays out a clear process for you and your vendor to follow. The dispute resolution provisions of an EHR contract are among the most important in order to ensure continuity of patient care and the health care provider organization's business operations. Dispute resolution clauses anticipate, as much as possible, problems that may arise during the parties' relationship. A well-drafted dispute resolution provision can help ensure that problems are satisfactorily resolved in a manner that is beneficial to you. Additionally, a dispute resolution clause can help to preserve the parties' relationship during challenging periods.

8.1 Negotiation and Escalation

Before taking formal steps to resolve a dispute under litigation or arbitration, which is discussed below, you and your EHR vendor will usually endeavor to come to a resolution through informal means. Your EHR contract can help you to achieve an informal resolution if it specifies some basic procedures to be followed if a dispute arises. For example, your EHR contract could create a window of time within which the parties are obliged to negotiate a resolution of the dispute and may require the senior executives of each party to meet to discuss the dispute before litigation or arbitration can begin. Your EHR contract also could require that the dispute be mediated as a preliminary step. Mediation allows an experienced mediator to work with both parties to try to negotiate a settlement in order to avoid litigation or arbitration. Typically the parties will share the costs of mediation. Mediation is not binding and a mediator does not "decide" the dispute. However, a successful mediation may involve the parties reaching formal agreement (enforceable as a contract) to resolve the dispute.

8.2 Litigation and Arbitration

If informal negotiation and mediation fail, then contract disputes are resolved either by a trial in a court, referred to as litigation, or through an out-of-court process agreed upon in the contract known as arbitration. In general, if your EHR contract specifies that disputes will be arbitrated, then you will be unable to take your dispute to a court, which may significantly limit the types and extent of relief to which you may be entitled. The following chart illustrates the major differences between these two approaches to dispute resolution:

Issue	Arbitration	Litigation
Who is the decision maker?	Determined by contract. Could typically be 1 or 3 arbitrators selected by an arbitration service or parties could agree on the arbitrator(s). Could require familiarity with health care and/or technology.	Judge is randomly assigned by court. There may also be a jury to decide factual questions.
Can the decision be appealed or is it final?	Generally final. No right to appeal even if a party disagrees with arbitration findings. Some feel that arbitrators tend to "split the difference" because there is no formal opinion and such opinion is not subject to review on appeal.	Decisions can be appealed (although easier to appeal judge's legal findings than jury's findings of fact).
Public or private proceedings?	Private—usually conducted in the arbitrator's office.	Public can attend, subject to certain exceptions. Court reporter prepares a transcript, which is usually a public record.
Scope of remedy	Arbitrator only determines damages to be paid. Winning party must then enforce in court if other party does not pay. Arbitrator not able to enter injunction or other orders. There are very limited ways to appeal.	Judge can determine liability and award damages. Judge can also compel action by an injunction or an order to do or stop doing something (e.g., provide access to data as required under the contract).
How much discovery will be allowed?	Parties often agree to limit number of depositions and witnesses. Given the increasingly complicated disputes being heard in arbitration (e.g., EHRs may be difficult for the finders of fact to understand) arbitrators are less likely to severely limit discovery of evidence or push parties to final trial in short time frames.	Rules of evidence apply. Broad discovery usually possible to obtain relevant information.

Issue	Arbitration	Litigation
Cost	Generally viewed as cheaper because limited discovery and no appeals. At times, it can be more expensive than litigation due to filing/administrative fees and arbitrator's fees paid by the parties that are not required in court.	More formal procedure may cost more (more extensive discovery). Appeal could add cost. May favor the "deep pocket" or a party who wants to delay payment.
Timing	Often faster but can drag out due to schedules of arbitrators and parties.	Depends on court's caseload, judge's approach to managing the litigation, and whether trial court decision is appealed.
Enforcement	There are some limitations on the arbitrator's authority and the enforceability of arbitrator's orders and judgments (which must be filed in court to be enforced).	Final judgment resolves the issues and determines the rights and obligations of each party. If one party fails to comply with the judgment, the other party usually will need to return to court to seek relief.

Whether litigation or arbitration is a better option in the event of a breach of contract depends on a number of variables, including your unique circumstances, business considerations, and preferences. The decision as to whether to include either a litigation or arbitration provision in the EHR contract should be discussed with an experienced attorney. For example, arbitration may be attractive to a party who wishes to maintain confidentiality of the dispute since the proceeding is not open to the public. Alternatively, only through litigation can you seek non-monetary relief, such as an injunction compelling your EHR vendor to take or cease a certain action (e.g., prohibiting the disclosure of a party's proprietary information). A model contract term that provides options for both litigation and arbitration can be found at the end of this section.

8.3 Ensuring Continuity of Service

Regardless of whether your EHR contract specifies informal negotiation procedures to be followed, or whether litigation or arbitration applies, you will usually need to use your EHR, and continue to receive support services from your EHR vendor, until the dispute is resolved. Therefore, your EHR contract should require the EHR vendor to continue to perform its obligations under the contract during any dispute so there is no interruption in access or services that could negatively affect patient care.

Because an EHR vendor would usually want this obligation to operate mutually, you should be aware that requiring continued performance may obligate you to pay for software or services that you believe do not satisfy the contract. If both parties decide to require continuing performance, then you should preserve your ability to terminate the contract if necessary to comply with any legal requirements.

A more favorable contractual position for you may be one that requires continuation of service while still:

- allowing you to withhold payment of disputed amounts until the dispute is resolved (e.g., disputes about how a rate schedule was applied); and
- permitting you to withhold all or a portion of payments for poor service.

An EHR vendor's standard form contract typically will not give you these additional rights, but these provisions may be negotiated between the parties. The model contract term at the end of this section includes language about continuity of service that you may wish to use, subject to you obtaining appropriate legal advice.

8.4 Other Contract Terms that Impact Dispute Resolution

Your EHR contract may also include the following terms that protect the vendor and pose additional barriers to a fair resolution of a dispute. You should consider carefully, with the advice of an attorney experienced in negotiating EHR contracts, the implications of terms that:

- permit the EHR vendor to terminate support or other services if there is a dispute, including for non-payment;
- allow the EHR vendor to charge late fees or interest on payments not made in full and on time regardless of whether the fees are disputed;
- require your claim to be made within twelve months or another period of time after the event giving rise to the claim arose (often a much shorter timeframe than the applicable statute of limitations that would otherwise apply);
- require the location of the litigation or arbitration to occur only in the EHR vendor's home state, referred to as "forum" or "venue" (if that venue will cause you inconvenience or additional costs); and
- provide that the laws of the EHR vendor's home state apply to the interpretation of the contract terms and its enforcement, referred to as "choice of law."

8.5 Costs

Many EHR vendor standard form contracts address the costs of dispute resolution. Under U.S. law, the losing party in litigation or arbitration generally is not required to pay the attorneys' fees and costs of the winning party ***unless*** the contract requires the loser to pay such costs. This means that if there is a claim and the EHR vendor eventually loses, you may not recover the fees and costs of litigation or binding arbitration, so you need to consider whether or not you wish to negotiate language that would require the losing party to pay such fees and costs. The downside of such language is that if you lose, then you would be required to pay the EHR vendor's fees and costs. The costs of litigation or binding arbitration can be significant and typically are not covered by insurance for breach of contract cases. The possibility of having to pay the other party's legal fees and costs may make it less likely for the party with fewer resources to pursue litigation or binding arbitration. You therefore should understand the practical effect of the dispute resolution terms on your ability to enforce your rights under the contract through either litigation or binding arbitration.

8.6 Example Dispute Resolution Contract Term

An example of a dispute resolution provision favorable to an EHR customer follows:

Example Contract Term 22

Dispute-Resolution Procedures. The parties hereto intend that all problems and disputes between them, of any nature, relating to this Agreement or arising from the transactions contemplated hereby, shall be resolved through the procedures of this Section; provided, however, that neither party shall be under any obligation to invoke the procedures of this Section with respect to disputes concerning any alleged breach that is not capable of cure. The procedures in this Section shall not replace or supersede any other remedy to which a party is entitled under this Agreement or under applicable law, and either party may take any legal action in a court of law or equity to assert or enforce a claim it has against the other party under this Agreement. Moreover, the procedures shall not be construed as an agreement to arbitrate or mediate any dispute. All expenses incurred by either party to resolve any dispute under this Section shall be and shall remain the responsibility of such party. The parties shall continue to perform their respective obligations during the pendency of any dispute, and the timeframes for such performance shall continue in full force and effect unless the parties otherwise mutually agree in writing. Notwithstanding the foregoing, Customer may suspend payment for the portion of the Services that is in dispute; all undisputed amounts shall be subject to the payment obligations set forth herein.

Negotiation and Escalation. The parties initially shall attempt to resolve disputes arising in the ordinary course of the parties' performance under this Agreement through the good-faith negotiation of the parties' project managers. If, after three (3) business days of good-faith negotiations, the parties have not been able to resolve any dispute, then each party shall prepare a written notice describing the nature of the dispute in reasonable detail and the attempted resolution ("Dispute Notice"), and shall submit the Dispute Notice to each party's appropriate senior-level executive, who shall attempt in good faith to resolve the dispute within five (5) business days from receipt of the Dispute Notice. If the parties have not been able, in good faith, to resolve the dispute following escalation of the Dispute Notice to each party's senior-level executive, then the parties may take any legal action in a court of law or equity to assert or enforce a claim it has against the other party under this Agreement. The final resolution of any such disputes between the parties hereto shall be reduced to writing.

Continuity of Services. Under no circumstance, including, but not limited to, the pendency of any dispute, may the EHR Vendor repossess or disable the Software, render the Software unusable, or terminate or suspend or limit any of its performance, or any licenses hereunder, including its duty to provide Services, unless and until Customer agrees in writing to such termination, suspension, or limitation, or a court of competent jurisdiction so determines.

[THE FOLLOWING TWO CLAUSES ARE MUTUALLY EXCLUSIVE OPTIONS AND YOU SHOULD SELECT ONE OR THE OTHER CLAUSE DEPENDING UPON YOUR PREFERENCE FOR EITHER LITIGATION OR ARBITRATION:]

[OPTION 1] Legal Action. If either party believes in good faith that the procedures described in this Section will have a material adverse impact on such party, then the parties may take any legal action in a court of law or equity to assert or enforce a claim it has against the other party under this Agreement.

[OR]

[OPTION 2] Arbitration. Any dispute arising out of or relating to this Agreement or the subject matter thereof, or any breach of this Agreement, including any dispute regarding the scope of this provision, shall be resolved through arbitration administered by the [American Arbitration Association (AAA) or the Judicial Arbitration and Mediation Service (JAMS) or American Health Lawyers Association (AHLA) Dispute Resolution Service] and conducted pursuant to the [AAA or JAMS or AHLA] Rules of Procedure for Arbitration.

9. TRANSITION ISSUES: SWITCHING EHRS

You may at some point need to consider switching EHRs if your existing EHR contract ends or your current EHR vendor:

- has not developed functionality that will enable you to comply with new regulations, quality reporting initiatives, or payment models;
- failed to disclose additional costs that must be paid to realize the full benefit of the EHR's functionality or limitations that have interfered with your ability to access or use the EHR's capabilities;
- did not provide agreed upon customizations that are critical to the manner in which you deliver patient services;
- provided a level of support services with which you are dissatisfied;
- was responsible for a security failure that had serious consequences for you organization or your patients;
- increased prices significantly when it was time to renew the contract;
- decided to discontinue support for your specific EHR (or exited the market entirely); or
- was acquired by another company that stops supporting your current EHR and wants you to switch to another EHR that you do not find acceptable.

You may also need to switch your EHR if you are unable to integrate its functionality with existing clinical workflows or if your business needs have changed so that your current EHR does not provide sufficient functionality to meet new clinical demands.

Switching EHRs can be costly and disruptive. It also presents a range of operational and clinical risks, not least of which is the significant risk that you will lose access to both patient and business records or that the data will be incomplete or corrupted. The significant costs of transition may include the cost of hiring external resources and the time your own staff will need to devote to the system conversion.

Some of these risks can be reduced by ensuring that you and your vendor discuss these issues at the outset of your relationship and negotiate appropriate transition provisions in your EHR contract. Unfortunately, very few EHR vendors include ***any*** transition provisions in their standard form contracts. As a result, you will typically need to negotiate with your preferred EHR vendor to include specific transition rights and obligations in your EHR contract to minimize the disruption and risk that might arise should you need to switch vendors in the future.

9.1 Length of Support Commitment

In addition to negotiating the inclusion of specific transition rights and obligations into your EHR contract (as discussed below), you can establish some basic protections against the risk and disruption of switching EHRs by ensuring that the duration of your EHR contract is appropriate and that you have options to renew at reasonable prices.

If your EHR vendor provides you with EHR software under license, your EHR contract will typically limit the period of time during which the EHR vendor will support the EHR. This is usually the case even if the contract grants you a "perpetual" license to use the software. The length of the vendor's support commitment effectively limits how long most customers will be able to use the software even if the license term is longer. For example, if the EHR vendor is no longer answering questions, fixing bugs, and providing enhancements for the software to comply with new regulations, most customers will need to find another EHR because they do not have the technical information or resources to take on those responsibilities.

Conversely, if your EHR is provided under a cloud-based EHR model, the service contract will be for a specified time period but will often contain automatic renewal periods. This means that the contract will continue in effect for the renewal period unless either party objects by a specific date. If you do not wish to renew, there is a risk that you may forget to object and find yourself locked into an automatic renewal period. You may therefore want to change the renewal period provision so that the EHR contract does not renew unless you give affirmative notice of renewal. If possible, the vendor would always be obligated to continue to provide the services in the renewal period so the decision would be solely up to you.

Different problems may arise if the EHR vendor has the right to not renew the EHR contract (or the support agreement for licensed software). If the period for notice of non-renewal is too short for you to find and transition to another EHR, the current EHR vendor can use this right as leverage to increase fees. For example, if the contract permits the vendor to give notice of non-renewal 90 days prior to expiration of the current term, would that be enough time for you to select and start transitioning to a new EHR? If the EHR vendor has been acquired by another vendor that now wants you to switch to another EHR, it may use its right of non-renewal to cause you to switch and possibly charge you additional fees. As a practical matter, you should keep close track of renewal dates and begin considering your options well in advance of when notices related to renewal must be provided.

In addition to negotiating the renewal provisions, you need to carefully evaluate the length of the initial term of the EHR vendor's services and support in both cloud-based and licensed EHRs. For example, at first you may want the initial support or service term to be short (to minimize your financial commitment). However, it may reduce your transition-related risk if your EHR contract obligates the vendor to support or provide services for a longer term if you decide to renew (at your sole option). The vendor may attempt to resist this contractual obligation by arguing that

you should in turn be committed to use (and pay for) the support or service for the same (longer) period that you are asking the vendor to commit to. Your counterargument would be that the EHR vendor will not incur much additional cost if you do not renew the support or services, as opposed to the very significant adverse impact to you if support or service is withdrawn.

It is beyond the scope of this guide to offer specific suggestions regarding pricing. However, you may wish to negotiate caps on future price increases upfront to limit the amounts that the EHR vendor may seek to impose for the renewal periods of the EHR service or support contract.

9.2 Commitment for Transition Services and Data Portability

There are many reasons you may find yourself transitioning from one EHR to another, but whatever the reason you are likely to need assistance to achieve a seamless transition. In some situations, it may be extremely difficult to have an effective transition without significant cooperation and assistance from your outgoing EHR vendor. An EHR vendor's willingness to agree to reasonable transition services should be a significant factor in your selection of an EHR.

It may be impossible to predict at the time you are negotiating your EHR contract exactly what transition services you will require, but it is important to at least obtain the EHR vendor's general agreement to provide a reasonable degree of transition assistance. Contract terms that support an orderly transition from your current EHR will structure, speed up, and simplify what can be a very time-consuming, expensive, and difficult process. While there may be a range of other transition details to consider, at a minimum you should try to negotiate the following terms:

(a) Software License

The EHR vendor should grant you the right to use the software during a stated transition period following the end of the services (for a reasonable stated fee if necessary).

(b) Transition Support Services

The EHR contract should require the EHR vendor to continue to provide support for the EHR during the transition period at the same level set forth in the EHR contract or, at a minimum, at the same level as received by other customers. This may be of particular importance if disaster recovery services are needed during a transition period.

(c) Data Transfer and Conversion

An outgoing EHR vendor should be required to provide assistance with transitioning data to a new EHR vendor's system. Your outgoing EHR vendor may store your EHR data in a format that is optimized for the vendor's proprietary system and which cannot be deployed into a new EHR without first being converted (sometimes referred to as data conversion). In the absence of a contractual obligation that specifies the EHR vendor's data transfer requirements, your outgoing EHR vendor may take the position that it can satisfy its obligations by providing you with all historical records in a format that is inconvenient or impractical rather than working with you in good faith to deliver the records in a standardized structure and format that is then generally accepted in the health IT industry. It is also helpful to specify a deadline for all data conversion so the implementation of your new EHR is not delayed by the outgoing EHR vendor unexpectedly providing the data in multiple batches over a period of weeks or even months.

The consequences of not reaching agreement on data transfer and conversion could be far reaching. For example, if your patient records are not provided in a format that makes them fully accessible in your new EHR, your health care professionals may be unable to rely on clinical decision support tools provided in your new EHR that use the old data such as automated drug interaction checking and allergy reminders. Further, if data is not provided in an appropriate format, you will incur the time and costs associated with converting the data to a usable format. When negotiating this requirement you may need to stress to your EHR vendor that if it is unwilling to agree upfront to providing appropriate assistance when transferring data to a new EHR, you will require that it provide you with access to the tools necessary to

undertake this work yourself. This may include access to the EHR vendor's data dictionary, database structure, or other intellectual property. See *Section 5 – Fostering Interoperability and Integration* for a discussion on obtaining access to information about the vendor's data structure or model.

9.3 Example Contract Language for Transition Services

The following language is a starting point in negotiating transition services, but it needs to be tailored to your specific situation with legal advice and possibly technical advice regarding the format of the data, length of time for transition services, and other details.

Example Contract Term 23

Transition Services
Upon the expiration or termination of this Agreement for any reason, EHR Vendor shall provide the services described below (the "Transition Services") for up to _____ (__) months if requested by Customer (the "Transition Period"). Transition Services shall consist of the following to the extent requested in writing by Customer:

(a) continuing to provide the Services required under this Agreement as of the date of termination (including applicable service levels and disaster recovery services), or such subset of such Services as Customer may direct; and

(b) providing all reasonable cooperation to Customer, its contractors and replacement EHR vendor(s) in order for Customer to transition its data to a successor system, including: (i) working in good faith to provide all data in a standardized format and structure that is then generally accepted in the health IT industry or is otherwise acceptable to the Customer; or (ii) assisting with the conversion of such data for use in a new EHR.

The parties shall negotiate reasonably and in good faith to agree on details of the Transition Services including the deadline for completion of data conversion services.

Transition Fees
(a) Subject to (b), the Transition Services shall be provided by EHR Vendor for the following fees: _____ payable as follows: _____. Such fees shall not exceed the then current hourly rates that would be charged by EHR Vendor for similar services provided under this Agreement.

(b) Notwithstanding the foregoing, in the event that the Agreement is terminated by the Customer on the basis of the EHR Vendor's breach of this Agreement, including a breach of the EHR Vendor's warranty that the EHR system is certified under the Current Requirements, then the EHR Vendor shall provide the Transition Services free of any fee, charge or set off.

Your EHR vendor may wish to include additional rights and obligations in any negotiated transition provision. For example, depending on the scope of transition services to be provided, your vendor may want a reasonable amount of notice of your need for transition services. It may also seek to limit the number of hours that it will commit to spend providing ongoing transition services. These concessions may be reasonable, provided they do not limit the vendor's core transition services obligations under the contract.

In addition, your EHR vendor may prefer not to specify a fixed price for transition services and instead provide that such services will be billed at the vendor's future prevailing rates. You should be aware that fees for data transfer and conversion vary widely across the industry and may increase significantly over the term of your contract. Therefore, if you do agree to accept a vendor's future prevailing rates instead of a fixed fee, you should stipulate an agreed-upon base price and/or rates and provide that any increases shall not exceed an agreed-upon amount.

Because transferring and converting your data may require providing third parties with access to software or documentation needed to map or convert data, your outgoing EHR vendor may require that the new EHR vendor sign a confidentiality agreement as a condition of gaining access to this intellectual

property. This may be acceptable so long as the confidentiality provisions are reasonably necessary to ensure the confidentiality of the outgoing EHR vendor's intellectual property and are not drawn in such a way as to frustrate your new EHR vendor's ability to access and facilitate the conversion of the EHR data.

9.4 Accessing Previous EHR Software

Software licenses typically require that you return all copies of the software and related documentation at the end of the license term. Similarly, cloud-based services agreements provide that services will end upon termination. These provisions are rarely negotiated but it is best practice to do so because you may need access to the software of your previous EHR in the future in order to respond to investigations or litigation. Possible exceptions to the obligation to return licensed software could be stated in an EHR contract for a provider-hosted EHR as follows:

Example Contract Term 24

Customer may retain a secure archival copy of the most recently used Software, all previous versions, and all documentation for use in responding to e-discovery requests for Documentation in its "native format."

Customer may use the archived software in litigation, arbitration, or government investigations regarding reimbursement, malpractice, or other matters in which the use of such items would help establish what information was known to Customer and its EHR users at the time in question and how it appeared.

The second paragraph above could be important to you in the defense of a medical malpractice claim since it may be necessary to use an old version of the EHR vendor's software to determine what information could have been available to a health care professional who reviewed a patient's records at a particular point in time.

If your EHR vendor provides the EHR as a service under a cloud model, you typically would not have received the software. Therefore the EHR contract should impose an obligation on the vendor to maintain copies of all software versions and to provide services to facilitate your access to the software in the circumstances discussed above. You could include a mechanism in your EHR contract to pay a reasonable amount for these services (if the vendor required).