October 2020 | Volume 14, Number 1

JOURNAL OF HEALTH AND LIFE SCIENCES LAW

OFFICIAL JOURNAL OF AMERICAN HEALTH LAW ASSOCIATION

AMERICAN HEALTH LAW ASSOCIATION

The mission of the AHLA *Journal of Health and Life Sciences Law* is to publish in-depth, professionally reviewed articles that are interesting and useful to intermediate and advanced health lawyers throughout the United States.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that the publisher and authors are not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.
—From a declaration of the American Bar Association

Consistent with the American Health Law Association's educational mission, it is an objective of the AHLA *Journal of Health and Life Sciences Law* to be a forum for the free expression and interchange of ideas. Contributors to the *Journal* are not agents of the American Health Law Association. The opinions and positions stated in the *Journal* are those of the authors and not of the American Health Law Association, its staff, volunteers, editors, or editorial board.

The AHLA *Journal of Health and Life Sciences Law* (ISBN 978-1-4224-4585-3. ISSN 1942-4736) is published three times per year by the American Health Law Association, 1099 14th St., NW, Suite 925, Washington, D.C. 20005. Telephone 202-833-1100. www.americanhealthlaw.org.

The reprint of American Health Law Association publications (including the *Journal of Health and Life Sciences Law*) is handled by the American Health Law Association. To request reprint permission (which will be addressed on a case-by-case basis), please contact Katherine Miller at kmiller@americanhealthlaw.org.

Subscriptions to the AHLA *Journal of Health and Life Sciences Law* are complimentary for members of the American Health Law Association. Paid subscriptions are available at www.americanhealthlaw.org/journal.

AHLA Diversity+Inclusion Statement
In principle and in practice, the American Health Law Association values and seeks to advance and promote diverse and inclusive participation within the Association regardless of gender, race, ethnicity, religion, age, sexual orientation, gender identity and expression, national origin, or disability. Guided by these values, the Association strongly encourages and embraces participation of diverse individuals as it leads health law to excellence through education, information, and dialogue.

Publication Staff

David S. Cade
Executive Vice President/ Chief Executive Officer
dcade@americanhealthlaw.org

Rob Anderson
Senior Director of Publishing
randerson@americanhealthlaw.org

Lisa Salerno
Director of Member Publications
lsalerno@americanhealthlaw.org

Katherine E. Miller
Senior Legal Editor, Member Publications and Resources
kmiller@americanhealthlaw.org

Annie Hsu Shieh
Citation Editor

Mary Boutsikaris
Creative Director
mboutsikaris@americanhealthlaw.org

Jen Smith
Graphic Designer
jsmith@americanhealthlaw.org

Practice Resource

Health Care IT Outsourcing: A Conundrum for Providers

Michael D. Rechtin, Chris DeMeo, Amy S. Levin, and Sheryl T. Dacso

ABSTRACT: As technology has moved from laboratory to industry, its role in commerce has evolved as a critically important and ubiquitous tool for not only individual interactions, but also in the delivery of health care services. Driven by health care regulations, economic survival, and quality standards, and currently by the COVID-19 pandemic, information technology (IT) has evolved as one of the most important components of the health care industry. Common IT functions include application/software development, web development/hosting, application support or management, technical support/help desk, database development/management, telecommunications, and other infrastructure support. Health care providers (Providers) now need to decide on a routine basis whether to provide IT services using internal resources and infrastructure or outsource those services to third party vendors. In making the decision to keep in house or to outsource, many competing interests need to be considered and weighed. Control is lost when ceding IT functions to outside providers, but with that loss of control comes the potential of cost savings and deep expertise in that IT function, which can yield operational benefits and create a competitive advantage. However, if there is a delegation of these IT functions to an outside vendor, the provider still retains the risk and responsibility for health care compliance as the legally accountable organization.

Michael D. Rechtin et al., *Health Care IT Outsourcing: A Conundrum for Providers*, J. Health and Life Sci. L., Oct. 2020 at 108.

Health Care IT Outsourcing

ARTICLE CONTENTS

INTRODUCTION

In the past, most Providers opted to manage their IT needs internally. Some used application service providers (ASP) to operate software that the Provider is given a right to use. Others used their own developed software or licensed software. With increasing expense, demand, and complexity in technology, for many, using their own software became impossible. Now, most Providers, no matter their size, outsource all or some of their IT functions to IT vendors. Commonly outsourced health care provider IT functions include services such as electronic health records, health information systems, revenue cycle management, pharmacy and lab information support, clinical decision support, hospital management systems, and e-prescribing, as well as administrative functions such as payroll and HR. The choice of which functions to outsource, and how that outsourcing arrangement will be structured, require foresight and coordination exercised in connection with the capabilities of each vendor.

CONSIDERATIONS FOR OUTSOURCING IT SUPPORT

IT support from a third-party vendor can come in many forms and differs depending on the IT goals and needs of the particular Provider. Recently, many companies have elected to utilize the "cloud" as a form of IT outsourcing, including software-as-a service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) engagements. Two common ways to use the cloud are either running one's software on computer servers owned by the cloud provider (so-called "hosting" arrangements) or storing data on the cloud provider's computer servers. A cloud could be a "public" cloud where the computer servers host the software or data using infrastructure that is shared among customers, or a "private" cloud where servers are exclusively dedicated to the needs and usage of one customer. Public clouds can be provided in conjunction with a third-party vendor which, as discussed below, can raise issues for information security to the extent the Provider does not have recourse against or bargaining parity with respect to that third-party vendor.

In addition, some IT service providers will take over the management of some of the Provider's IT functions, such as call center support, which will free up time for the Provider's IT team to focus on core business issues or operate more leanly. For example, one form of IT outsourcing arrangement could be what is generally referred to as a "traditional" IT outsourcing arrangement using, for example, offshore vendors in countries such as India, which are engaged to provide a customized bundle of IT services to the Provider. Another form of IT outsourcing arrangement could involve the use of standardized infrastructure, platform, or software tools through the "cloud."

Workforce restructurings and internal budget constraints may also drive Providers to engage third parties to perform IT services as opposed to using internal resources. Unlike the internal IT team of a Provider, the IT service provider may have more highly specialized talent, increased operational resiliency, better economies of scale, a diversified geographic footprint, and access to different and unique types of technology that are unavailable to the

Provider except through a third-party vendor. Outsourcing may also enable the Provider to use "big data" techniques, in compliance with the Health Insurance Portability and Accountability Act (HIPAA) and other patient information privacy laws at the state and federal level, to data-mine for patterns and tap into the increasing power of artificial intelligence and machine learning.

Integrating the insourced and outsourced IT functions across multiple software and cloud-enabled, or Provider-owned hardware, is often very complex; especially for large, sophisticated systems. Outsourcing may take the form of one-off software programs or, more likely, entire broad IT functions being outsourced to one or more IT vendors. Many Providers, large and small, utilize the services of consulting firms when considering or making these changes.

The contractual arrangements underlying these outsourcings can be hyper-technical. Many contain unfamiliar industry-specific business and legal terms and regulations that can result in unintended consequences if not properly understood or negotiated. Often times, these agreements are drafted in a very "vendor-friendly" manner, which leaves the Provider without important rights, remedies, and protections. For these reasons, Providers looking to outsource their IT functions should consider utilizing internal and external attorneys who have significant experience and subject matter expertise in both technology and health care regulations.

This article will discuss IT outsourcing, including the anatomy of an IT outsourcing contracting cycle, items to be aware of in negotiating those contracts, and issues to be most concerned about through the lens of Providers, and the particular legal and regulatory challenges they face. The outsourcing process typically starts with the Provider having a need that is not currently being met. This need could take the form of a new and necessary technology, a modification to an existing technology, a business requirement, a new platform, external business pressures to keep up with the competition, or internal business pressures such as the need to cost save or otherwise comply with regulatory requirements. IT needs are rarely static and are instead dynamic and constantly changing. The COVID-19 pandemic has greatly increased the use of technology by Providers who rely on virtual technology to allow continued access by patients to providers who can work from home or office to reduce exposure and disease spread. The need to expand technology has created new and unforeseen demands on Providers that, in many cases, must be outsourced because of cost and specialized systems support. This unprecedented explosion in need, combined with little time to react, makes it difficult for the Provider to consider and analyze fully the outsourcings and their related contractual agreements and properly review all the issues that should be considered.

CONSIDERATIONS FOR CONTRACTING

Many IT outsourcing contracts tend to be opaque, dense, and not user friendly. Depending on the budgeted amount to be spent and number of functions to be included on the outsourcing, the contracts themselves could be negotiable. However, some types of contracts, such as electronic health record (EHR) vendor agreements, may be more difficult to negotiate with

the larger size vendors.[1] Higher revenue contracts, including contracts that provide for a guaranteed spend over a fixed period of time, may give the Provider more leverage in negotiations. In all cases, IT outsourcing contracts will have language within them that needs to be identified and negotiated in the interest of the Provider's requirements. This necessitates that the Provider have a skilled legal team involved in the review of these contracts, with both health care and IT expertise.

When an IT need is identified, the Provider should consider whether one of its incumbent IT vendors could fulfill this need, or whether it makes sense to go to the market for the relevant services. Despite any existing relationship, and depending on the type of IT services involved, for significant or complex IT outsourcing arrangements, the Provider may want to commence the process using a request for information (RFI) from which a list of the best IT vendors can be identified based on an optimal solution at the best price (whether a new service or expansion of an existing service.) Some providers may choose to engage a health care IT consulting firm to assist in the process of developing the RFI to be issued to several potential vendors in order to identify the breadth and experience of those vendors based on the function to be outsourced. The RFI process will then lead into the more detailed request for proposal (RFP) that will outline the needs, goals, issues to be considered, contract terms, and anything else the Provider team deems important to its delegated vendor functions and be prepared by, or with input from, the health care IT consulting firm. The RFP process naturally results in a reduced list of vendor candidates and it is at this point that the Provider can drive better deal terms through the competitive bidding process. If the IT vendor has no business relationship with the Provider, it may offer better terms to get a "foot in the door."

This down-selection process often leads to an exchange of proposals and counter proposals describing detailed business terms for the transaction and ultimately the selection of a vendor, or possibly multiple vendors to combine efforts, contingent on the desired outcome. Depending on the scope of the IT outsourcing, at a minimum, legal counsel must be involved in the process, working closely with the internal business, procurement, and IT functions, as well as external IT consultants, project managers, and other professionals that are experienced in negotiating the necessary business and legal terms.

CONSIDERATIONS FOR CONTRACT TERMS AND NEGOTIATIONS

Once the Provider has selected the IT vendor, the parties will need to determine the contracting strategy and process. IT vendors, particularly cloud providers, almost always prefer to use their own form contracts. However, for more complicated outsourcing deals, and particularly for clients with greater leverage, the Provider may be able to create the first set of contracts that will govern the IT outsourcing transaction. It also may be possible to leverage an existing agreement with an incumbent vendor (amending only specific terms as needed) in order to

1 Common larger vendors include, but are not limited to, those such as eClinical Works, Allscripts, Epic, Cerner, and Athena.

streamline the contracting process. A non-binding term sheet or letter of intent should also be considered at the outset of the contracting process, particularly for more complex arrangements, in order to come to agreement on key terms and reduce negotiating time. When developing and drafting the contracts, consideration should be given to creating contractual incentives to reward vendor performance over benchmarks. These incentives are a counterbalance to the remedies a Provider has if the vendor fails to satisfy the Service Level Agreement (discussed in detail below) and helps create a better partnership between the Provider and IT vendor. The incentives could be in the form of sharing demonstrable savings achieved by discrete aspects of the outsourcing (such as rebadging Provider employees as vendor workforce) or additional payments if, for example, the vendor is able to achieve a monthly help desk complaint number below an objective metric. These need to be thoughtfully drafted so as to not create unintended consequences and capped so the Provider has certainty as to what the potential additional exposure is. Without incentives, the vendor is financially motivated to provide the services at exactly the levels described in the contract while minimizing its expenses in doing so. If the services are provided only at or slightly above the minimum level, that may be fine with the Provider; however, depending on what the service is, it may not be operationally acceptable with the Provider (such as chronic trouble with the help desk), but is otherwise not actionable under the contracts. By going into the relationship with an incentive payment feature, the vendor will be motivated to provide enhanced service to earn those payments and will be less likely to cut corners to achieve greater cost savings.

It is also important that both parties anticipate common problems or friction points that may arise during the term of the contract, and proactively address those points to the extent possible. For example, a common friction point that many customers encounter is that their IT needs and/or usage will fluctuate over time. The outsourcing contract should account for this, and address how pricing terms, service levels and other operational considerations will be adjusted as the customer's IT needs change. Similarly, another common problem is that many service providers require a certain degree of flexibility in how they perform the services (for example, service locations / use of off-shore resources, use of sub-contractors), which in turn enables the service provider to offer a lower price and protect its margins. However, from the customer's point of view, it may not be acceptable to give the service provider the authority to change service locations or engage third-party sub-contractors without the consent of the customer. Regulatory requirements that apply to the customer also may influence the parties' approach on these issues. Hence, this is a common friction point during the contracting process that will need to be thoughtfully addressed.

Another common problem that could arise, depending on the nature of the IT contract at hand, is the issue of intellectual property and the associated ownership rights of each party. The contract needs to be very clear as to exactly what intellectual property rights are owned by both the customer and the service provider. Depending on the arrangement, the parties also may decide to jointly develop technology solutions, in which case it may be prudent to enter into a separate development agreement to document in greater detail the exact rights of each

party in the relevant intellectual property. It also may be appropriate to structure the IT contract as a so called "work-for-hire," in which case the service provider would assign any and all intellectual property rights to the customer. For customers or service providers with operations outside of the United States, consideration also needs to be given to the intellectual property laws of the relevant jurisdictions, since many follow a different framework than the United States. In short, consideration of intellectual property rights and issues is very important and should be thoughtfully drafted at the outset of any IT outsourcing contract.

The following graphics will give you an idea as to what this documentation may look like for a traditional IT outsourcing arrangement: Figure 1 below illustrates a Master Service Agreement (MSA) contracting regime with the various Master Statements of Work and Statements of Work that are derivative of the Master Statements of Work and Schedules; Figure 2 on page 115 illustrates the less complex contracting structure of a Master Software License Agreement, and Figure 3 on page 115 illustrates a Services Agreement (Cloud Infrastructure); however, the process and type of contracts will ultimately depend on the type of IT function and the structure of the outsourcing arrangement.

Figure 1. Master Service Agreement

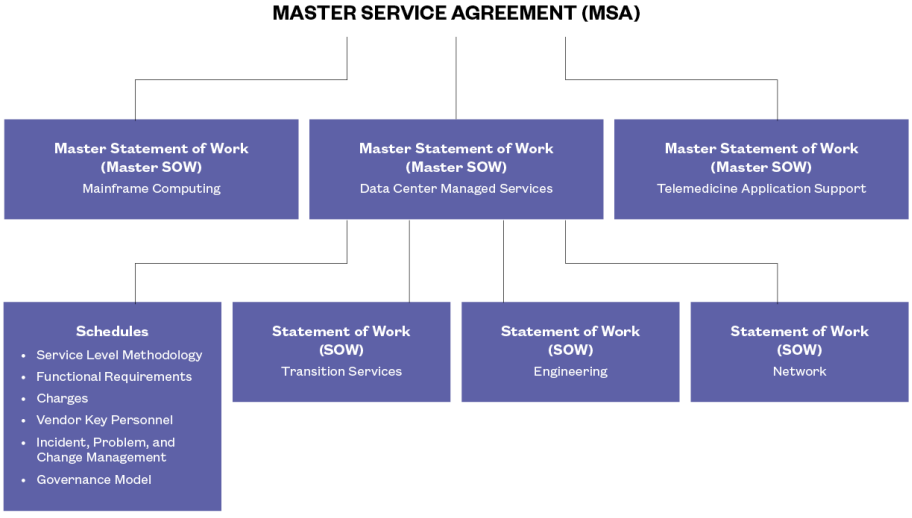


Figure 2. Master Software License Agreement

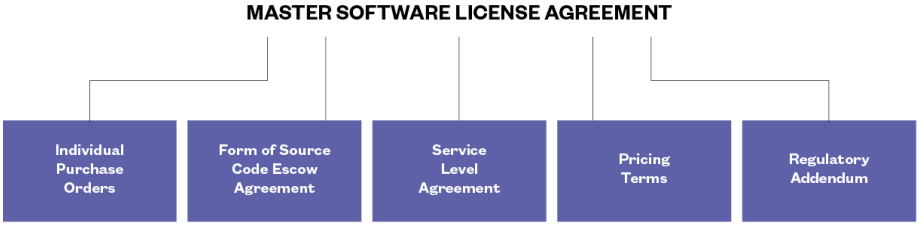
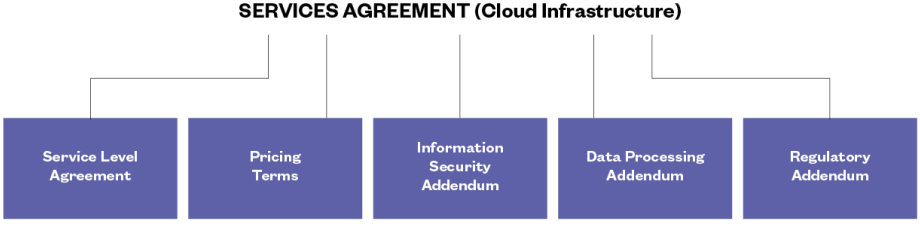


Figure 3



The Master Services Agreement

For traditional outsourcing deals, the Master Service Agreement or "MSA" is typically the primary and controlling document between the Provider and IT vendor and covers the general contract terms under which the parties will engage. If the outsourcing is sufficiently multi-faceted, beneath the MSA may be one or more Master Statements of Work (also referred to as a "MSOW") or Engagement Schedules. In the more complex situation with Master Statements of Work, an individual Master Statement of Work will cover one discrete portion of services, such as infrastructure services, application maintenance and support services, or help desk services. The Master Statement of Work or Master Service Order, as the case may be, will have specific Statements of Work or Service Orders that "branch off" that document, which specific Service Orders will describe in detail the particular services and economic terms of the different facets of the IT outsourcing. For example, an individual Service Order could describe the specific services and related pricing around main frame computer monitoring. Attached to the MSA or each Master Service Order, in addition, will be schedules that will cover a variety of items such as pricing methodology, governance,

transition terms, benchmarking, service levels and associated credits, workforce requirements, information security terms, and functional requirements. The MSA and the Master Statements of Work (including associated schedules) are binding legal documents, and attorneys will be primarily responsible for drafting and negotiating these documents with extensive involvement of the client. The detailed specific Service Orders and schedules are often prepared by the IT vendor with input from the Provider or the Provider's consultant. The party that prepares these documents and negotiates them is typically very fluid, and in many cases outside counsel to the Provider will draft and negotiate all of these documents, including the specific Service Orders.

For other types of outsourcing arrangements—such as IaaS, PaaS, SaaS, or software licensing agreements—a services agreement, with associated attachments, may be appropriate. For example, in a software licensing arrangement, the parties will typically negotiate and sign a software license agreement that will detail the scope of the license grant, pricing, usage terms (including restrictions), warranties against IP infringement, and other legal and business terms. These arrangements also usually involve entering into an escrow agreement with a third-party escrow agent whereby the vendor will agree to place the source code into escrow, which is accessible by the Provider if the vendor becomes insolvent, goes out of business, or other specified scenarios occur.

With regard to the cloud, the contracts governing these types of arrangements can vary widely. For example, cloud infrastructure or "IaaS" contracts are typically short and focused documents, particularly in the context of public cloud. In this case, cloud providers often utilize a "one-to-many" model, which involves a standardized set of terms that the provider will be highly resistant to negotiating. Service Level Agreements and pricing terms are also similarly standardized and typically non-negotiable, unless the customer has an unusual amount of leverage or is willing to make a significant financial commitment over a fixed period of time.

However, in all cases, because these legal documents cover important and strategic functions of the Provider, at a minimum, these need to be understood by the Provider's business team, relevant stakeholders, and the in-house lawyers who will be responsible for administering them.

Negotiation with some IT vendors may be challenging depending on the nature of what is being outsourced and the leverage the Provider has with the vendor. However, in all cases, it is very important to identify upfront the Provider's goals and needs from a business perspective—and to be clear about what is being agreed to. For example, in the context of traditional IT outsourcing arrangements that cover infrastructure support, there are many factors in the contract that affect the vendor's charges for the relevant services, equipment and support. The compensation metric can take the simple form of a fixed fee payable on a monthly basis or a more complex negotiated sum per "unit." The units can describe anything that can be measured, such as the number of IT vendor employees devoted to a task outlined on the Service Order multiplied by the amount of time each worker (say a call center in India)

spends devoted to this task or the amount of data storage being used in a cloud datacenter. When compensation is calculated based on units, the parties will use an estimate of "unit usage" to derive an anticipated monthly amount that will serve as the baseline monthly fee at the inception of the contract term, which will then be adjusted after the end of each month or other designated time period to account for either reductions in the amount of units used (so-called "RRC," for reduced resource credits) or additional units used (so-called "ARC," for additional resource credits) where a credit is then given to one party or the other for the following month (or other designated time period). If the scope of a service is changed or RRCs or ARCs are consistently given because the initial or any subsequent estimate of units was inaccurate, the parties may choose to modify the baseline amount. This can get complicated quickly in a legal document, so understanding the way in which the IT vendor will be paid—along with the calculation of ARCs and RRCs and ensuring that both sides understand the calculation (possibly with examples built into the legal document)—are critical so that there are no surprises in the future when the service starts and invoices are issued.

Another important issue is the locations and facilities where the IT vendor will be delivering the services. These are usually termed as either "onshore," "nearshore," or "offshore." Onshore would be the United States, nearshore would a vendor located outside of the United States but in a nearby time zone (such as Canada), and offshore would be India or another country. India has typically been a dominant player in the offshore IT outsourcing market for more traditional types of arrangements in part due to the availability of high-quality developers and other IT professionals at competitive cost. Many businesses, however, particularly those in regulated industries, are seeking to reduce or diversify their IT footprint coming out of COVID-19 (i.e., a desire to mitigate potential COVID-19 disruptions by limiting the number of countries where services are being performed to only those countries that have had demonstrable success containing the pandemic), widespread stay-at-home orders, and other governmental restrictions that could impact services. These factors could cause IT vendors to shift service locations to onshore and nearshore. In the past, companies would perform due diligence on IT vendors in the form of vendor site visits and in-person interviews, but in the current COVID-19 world, this has become difficult, if not impossible.

Service Level Agreements

Service Level Agreements (SLAs) are a part of most IT outsourcing contracts and are designed to incentivize the vendor to perform the services promptly, properly, and in accordance with all relevant legal and business terms. Often times, the SLAs will provide the Provider with remedies in the event the IT vendor does not satisfy certain very specific metrics that are written into the SLA, e.g., system up and running 99% of the time without incident or proactive response to urgent requests within one hour. The service levels themselves are typically tied directly to the services the Provider is paying for, so if the Provider opts for more offshore than nearshore, and consequently a longer time for the IT vendor to correct a problem, that will be reflected in the price charged but also the specific

service level promised in the SLA. If the SLA terms are then not satisfied, credits are given from the IT vendor to the Provider against future amounts owed on the contracts, which are typically capped at percentages of fees the Provider paid to the IT vendor, often called the "at risk amount."

The Provider's ability to outsource services may be constrained by regulatory requirements. For this reason, it is important for the Provider to determine its IT outsourcing goals at the outset and then craft its contracting strategy around what services must be handled onshore and what additional legal obligations arise when services are provided offshore. In such circumstances, the IT vendor will need to satisfy regulatory requirements and the contract need to offer the Provider remedies if the vendor breaches this requirement. The Provider should also have broad audit rights in the contracts so as to satisfy internal requirements and external regulatory and legal requirements related to compliance. Audit rights, typically in the context of cloud arrangements, can be very difficult and contentious provisions to negotiate with IT vendors, which for security and operational reasons are often reluctant to grant customers broad audit rights. Many vendors will also encourage customers to rely on third-party audit reports and certifications, such as SOC reports and ISO certifications, in lieu of direct or physical audits.

The ongoing COVID-19 pandemic has added additional scrutiny to force majeure provisions, which have long been overlooked during contract negotiations. It is very important to read these provisions closely and push back on terminology that gives the IT vendor broad discretion to trigger a force majeure event for circumstances "beyond its control." Seasoned IT vendors also have in place, and will continue to have in place, business continuity plans or disaster recovery plans that are designed to ensure that the vendor can continue to operate, satisfy the SLA requirements, and provide their services without interruption in the event of force majeure type events or pandemics. These plans have particular application for Providers' obligations under HIPAA to maintain the integrity and availability of protected health information (PHI). Providers should make sure that they include in the contracts that those business continuity and disaster recovery plans exist, will continue to exist at all times at the same or greater level than what are in place at the inception of the contract, and that the Provider has the right to periodically review them and rely upon them in a regulatory audit.

Cyber security and information security terms in these contracts are also extremely important, even more so in the face of COVID-19, and it is imperative to require that service providers carry and pay the cost of cyber liability insurance. In this regard, the MSA should require the vendor to procure insurance through an insurer approved by the Provider and in amounts that are appropriate in light of the risk involved. The Provider should also require that it be included on the policy as an additional insured and be notified directly if there are any changes in policy coverage.

The insurance provisions should further be drafted with an eye toward indemnity in favor of the Provider. Although federal HIPAA regulations do not provide a private cause of action for injured patients, many state laws do. Utilizing boilerplate indemnity provisions that are

limited to indemnification for third-party injury claims will not suffice. Instead, the indemnity provisions should also expressly cover regulatory investigations, penalties, and liabilities, as well as the vendor's compliance with applicable laws. There should be consideration of cyber-insurance coverage as well.

Because of the nature of these contractual arrangements, these documents may continue in effect for a long time. Specifically, the MSA should be designed to encompass future master service orders or service orders. It is important that the MSA be as "future-proof" as possible and provide flexibility; however, the parties also need to be willing to revisit them in the future when new services are added. For example, MSAs often will include a benchmarking schedule that outlines the process for when and how the customer can adjust the pricing depending on market conditions.

It should be noted that once certain IT functions are outsourced, it can be very difficult to unwind those relationships (the so-called "lock-in" effect), especially if the IT outsourcing involves the vendor providing software or hosting services, or other mission-critical services. Providers become reliant on these services and need to make sure there is an exit strategy and that pricing is protected long term. For these reasons it is important to understand that the likelihood and consequences of terminating these agreements, even if the IT vendor is in default, may not be something that the Provider will want to or can do because of the potential for disruption in operations. To protect the Provider, in addition to the right of termination and step-in rights (which allow the Provider to "step-in" and perform the services itself or through a third party), the Provider should also have different contractual remedy levers to improve the performance of the IT vendor. In some respects, this begins to look more like a strategic partnership than a contract.

In the event of a termination, however, it is critical that the agreement contain provisions for the orderly transition of data and services to the new vendor in a format and medium agreed to by the Provider. This issue can be hotly contested because vendors generally want to secure payment before releasing data. Because the potential legal and patient care risks for the Provider are greater and more difficult to remedy than non-payment, it is reasonable to insist on data and service transition provisions that favor the provider.

HEALTH CARE COMPLIANCE CONSIDERATIONS

As with all contractual arrangements involving Providers, IT outsourcing arrangements must be drafted and negotiated in the context of the panoply of statutes, regulations, licensing rules, accreditation standards, and billing and payment requirements that govern the provision of health care services. The compliance burden of a particular arrangement will depend on the scope of services. In this section, we endeavor to identify and provide a brief overview of the health care specific legal issues that will likely impact most transactions. Knowledge of these issues is particularly important when dealing with an IT vendor with little or no experience in health care transactions. The fundamental contracting strategy is to secure representations, warranties, and indemnifications from the IT vendor that foster compliance.

HIPAA and Related Data Privacy and Security Laws

The primary regulatory consideration for a Provider in outsourcing IT functions is the privacy and security of patient information. Addressing this issue begins with HIPAA. HIPAA governs the use and disclosure of PHI by covered entities and Providers, which includes information (in any form or medium) that identifies an individual, or can be used to identify an individual, and relates to the individual's health, health care, or the payment therefore.[2] As it relates to IT outsourcing contracts, Providers must implement administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of electronic PHI.[3] The IT outsourcing arrangement implicates each safeguard: the contract—and the Provider's rights and remedies—will be reviewed as an administrative safeguard; the cloud, SaaS, PaaS, and IaaS arrangements will be scrutinized as a technical safeguards; servers and other data housing functions implicate physical safeguards. The Provider should give special attention to whether a particular offshore arrangement ensures appropriate physical safeguards.

In addition, covered entities must ensure PHI is available to the individual for purposes of review and amendment,[4] and to the Department of Health and Human Services (DHHS) for purposes of confirming HIPAA compliance.[5] These obligations should set forth the IT vendor's duties and covenants under the contract.

Importantly, HIPAA also reaches the IT vendor as a "business associate." From the Provider's perspective, HIPAA generally allows a covered entity to disclose PHI to a business associate if certain regulatory requirements are met.[6] From the vendor's perspective, the HITECH amendments to HIPAA require that business associates comply with the same administrative, technical, and physical safeguards as covered entities.[7] These obligations and other HIPAA compliance matters are addressed in a Business Associate Agreement (BAA) that will be an addendum to the IT outsourcing agreement. The HIPAA regulations at 45 C.F.R. Part 164, Subparts C and E dictate the provisions that a BAA must contain,[8] but Providers should resist the urge to tack on a boilerplate BAA as an afterthought to the business provisions. The nature of an IT outsourcing transaction warrants a BAA that is tailored to the specific risks presented and integrated with the main contract.

IT vendors often attempt to shun these compliance obligations by claiming they are not a "business associate." Even in the most basic IT outsourcing agreement with a Provider, PHI is involved, which means that the IT vendor will need to sign a BAA. The general standard for

2 45 C.F.R § 160.103 (2020).
3 *Id*. §§ 164.308, .310, .312.
4 *Id*. §§ 164.524, .526.
5 *Id*. § 160.310.
6 *Id*. § 164.502(a)(3).
7 42 U.S.C. § 17931(a) (2020).
8 45 C.F.R §§ 164.308(b), .314(a), .504(e).

determining whether an IT vendor qualifies as a business associate is whether the vendor only transmits PHI from one point to another as a "conduit" or provides other services involving the use, maintenance, and disclosure of PHI.[9] The former category of vendor is not a business associate, while the latter, including a vendor who assumes part or all of a Provider's IT functions, is.

The HIPAA regulations also contain obligations for responding to internal and external incidents that compromise PHI, i.e., "breaches," that are applicable to both covered entities and business associates.[10] In addition to the baseline regulatory requirements regarding timing of notification, the Provider should carefully negotiate provisions regarding cooperation and allocation of responsibility and cost for a breach response.

In addition to HIPAA, state laws can provide additional requirements for the privacy and security of patient information. HIPAA does not preempt state laws that are more restrictive. As a result, many states have implemented laws that protect patient information. The law governing a patient's health information will generally be that of the state where the patient is located when receiving the services. Providers active in multiple states should ensure the IT outsourcing arrangement complies with applicable state law in each jurisdiction covered where they provide services and each jurisdiction covered by the agreement.

In addition, the Federal Substance Abuse and Mental Health Services Agency (SAMHSA) governs certain information relating to substance use disorders under 42 C.F.R. Part 2 (the "Part 2 Regulations"). Although recent waivers in response to COVID-19 and further reaching regulatory efforts have endeavored to make the Part 2 Regulations consistent with HIPAA, no permanent solution has been achieved. As such, IT outsourcing for Providers treating substance use disorders must account for compliance with the Part 2 Regulations.

Finally, nearshore and offshore arrangements may implicate foreign information privacy laws such as the European Union's General Data Privacy Regulation and Canada's Personal Information Protection and Electronic Documents Act. In negotiating for the potential impact of these laws, Providers should insist that the IT vendor assume sole responsibility, including indemnification, for compliance with these laws.

Medicare Requirements

Providers that participate in Medicare have additional considerations when it comes to IT outsourcing. For example, these providers may not contract with persons or companies that have been excluded from Medicare and must, therefore, review the DHHS Office of Inspector

9 *See, e.g.,* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5571–72 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 & 164).

10 45 C.F.R. pt. 164, subpart D.

General (OIG) List of Excluded Individuals and Entities to ensure that the IT vendor and any known subcontractor is not excluded by the OIG.[11]

If a Provider contracts with an individual or entity who is excluded by the OIG from program participation for the provision of items or services reimbursable under such a federal program, the provider may be subject to civil monetary penalty (CMP) liability if they render services reimbursed, directly or indirectly, by such a program.[12] CMPs of up to $20,000 for each item or service furnished by the excluded individual or entity and listed on a claim submitted for federal program reimbursement, as well as an assessment of up to three times the amount claimed and program exclusion may be imposed.[13] Providers have an affirmative duty to check the program exclusion status of individuals and entities prior to entering into contractual relationships, or run the risk of CMP liability if they fail to do so.[14]

Providers that contract with Medicare Advantage Organizations (MAOs) and/or Medicare Part D Plan Sponsors (PDPs) have additional obligations when contracting for offshore IT services. Specifically, the Centers for Medicare and Medicaid Services (CMS) requires that MAOs and PDPs provide attestations regarding offshore entities they contract with for "Medicare-related work" involving PHI.[15] These attestation requirements apply to contracted Providers and their subcontractors. MAO and PDPs push these requirements down through their provider contracts, which either prohibit the use of offshore contractors for Medicare-related work or require attestations from the provider regarding offshore vendors. As a result, IT outsourcing contracts should prohibit the use of offshore subcontractors for Medicare-related work or require representations, warranties, and certifications regarding offshore subcontractors.

Given the fundamental aspect of these legal requirements, and others that may be implicated in a particular transaction, Providers should not postpone the regulatory review until after all contractual terms are set. Instead, they should consider them when developing the IT outsourcing strategy and carry that strategy through the design of the outsourcing program, selection of vendor, and contract negotiations.

---

11 OIG, Updated Special Advisory Bulletin on the Effect of Exclusion From Participation (May 9, 2013), https://oig.hhs.gov/exclusions/files/sab-05092013.pdf [hereinafter Special Advisory Bulletin]. in Federal Health Care Programs

12 42 U.S.C. § 1320a–7a(a)(6).

13 42 U.S.C. § 1320a–7a(a)(6); 42 C.F.R. § 1003.102(a)(2).

14 Special Advisory Bulletin.

15 *See* Memorandum from David Lewis, Dir., Medicare Advantage Grp., Ctr. for Beneficiary Choices, CMS, DHHS & Cynthia Tudor, Dir., Medicare Drug Benefit Grp., Ctr. for Beneficiary Choices, CMS, DHHS to All Current and Prospective Medicare Advantage Plans, Prescription Drug Plans, Cost Plans, PACE, and Demonstration Orgs., Sponsor Activities Performed Outside of the United States (Offshore Subcontracting) (July 23, 2007), https://www.hopkinsmedicine.org/johns_hopkins_healthcare/downloads/amd/offshore_subcontracting_attestation.pdf.

CONCLUSION

Health care IT outsourcing arrangements are more important in today's environment than ever before. These arrangements require prior planning that should involve internal and external resources to ensure that the outsourced needs have been identified, the process for vetting vendors is determined, and the contracts are appropriately structured and effectively negotiated. There are many considerations involved with outsourcing and service agreements that should be undertaken as part of an organization's procurement process. Board engagement may be appropriate since many of these contracts are very expensive and budgetary considerations are necessary.

Each type of outsourced service raises different issues that must be planned and integrated into the procurement and contracting process. As we continue to endure the COVID-19 pandemic and our new normal involves increased reliance on technology to meet the public's health care needs, those in the health care industry must address how to continue to deliver appropriate care in a manner that meets both quality and legal standards.[16]

16 Press Release, Seyfarth Shaw LLP, Seyfarth Publishes New Treatise: The Future of Health Care in the US: What a Post-Pandemic Health Care System Could Look Like (June 16, 2020), https://www.seyfarth.com/news-insights/seyfarth-publishes-new-treatise-the-future-of-health-care-in-the-us.html.

CHECKLIST OF KEY ISSUES AND CONSIDERATIONS (NON-EXHAUSTIVE[17]) – IT CONTRACTING

Contract goals, form and structure. At the outset of any IT contract, it is important to determine the goals as well as the form of contract(s) that will be used, and the basic structure. For example, a Master Services Agreement may be used as the "main" agreement, which could have a number of different SOWs and schedules that sit underneath it.

RFI or RFP. Because IT contracts often support essential functions in a health care organization, it is a best practice to develop a request for information/proposal based on the desired goals, budget, and other requirements. It is also a good idea to check for regulatory guidelines that may apply to the particular type of contract.[18]

Non-binding LOI. For complex IT contracts, consider whether it makes sense to enter into a non-binding letter of intent before entering into detailed contract negotiations. This can save time and streamline the contracting process significantly.

Pricing terms. Pricing terms must also be clearly identified and documented in the contract. Different types of IT contracts will require different pricing terms and structures. For example, a software license agreement may provide for tiered pricing (based on usage), or flat-fee pricing on an enterprise-wide basis. Cloud services agreements are likely to include pricing terms calculated based on usage. Traditional ITO arrangements may include a variety of pricing structures, including pricing based on the number of service provider employees performing the work (known as FTE pricing) or could also be based on a flat fee that is adjusted up or down depending on usage / other metrics.

Contract term and renewal periods. The contract term and any renewal rights should also be clearly agreed and defined in the contract. Some contracts may provide for a fixed term (such as 3 or 5 years), and others may continue indefinitely until terminated.

Termination rights. Termination rights for the service provider and the customer should be clearly defined in the contract (and typically termination rights in favor of the service provider are much more limited). Common termination provisions include the right to terminate in the event of material breach of contract and/or specified insolvency events, which may include a cure period. Termination for convenience, coupled with a notice period, may also be appropriate.

Service levels and credits. For those services that can be objectively measured, the vendor should offer the Provider service level agreement language specifically identifying

17 In the context of health care, IT covers a broad range of administrative and clinical areas ranging from the information systems and their connectivity to patient monitoring, clinical data capture, and revenue cycle management. There is no "one size fits all" checklist, but our list seeks to provide general items that should be considered in any health IT contract.

18 For example, for electronic health records (EHR) vendor selection, the National Learning Consortium (NLC), under the auspices of HealthIT.gov, developed a set of tools to assist health care providers and IT professionals working on implementation, adoption and meaningful use of certified EHR systems.

verifiable metrics around those services that if not satisfied will give the Provider monetary remedies and termination rights. These service level agreement rights are often the sole remedy provided for breaching the service levels and are capped at a small fraction of the contract sums paid the vendor.

Transition terms. The parties should also consider whether "transition-specific" terms need to be identified and agreed upon in the contract (often, as part of a "transition schedule") to account for how the IT services will be transitioned from the customer to the service provider. Often times, the transition schedule will include key milestones and payments, and will refer to a more detailed plan to be jointly developed by the parties.

Statements of Work. Depending on the contract structure, technical specifications and business requirements may be set out on one or more statements of work that are attached to a master services agreement. These statements of work often require detailed business input and contain largely technical or non-legal terms.

Data privacy and information security terms. Data privacy and information security terms are critical considerations in any IT contracting arrangement and should be reviewed with specialist legal counsel. It is important that the parties consider where the services will be performed, what type of data and information will be shared, and what access rights the service provider will have, among other things.

Employment. Depending on the specifics of the IT contracting arrangement, employment considerations may be important. For example, if employees of the customer are transitioning to employment with the service provider (known as "re-badging") then a number of employment-specific terms and issues will need to be worked out with the assistance of employment counsel.

Business Associate Agreement (BAA). Although the HIPAA Privacy Rule and Security Rule dictate most of the terms of a BAA, the scope and risk associated with IT contracts require that the BAA include additional terms that protect the health care provider. Because the provider bears most of the risk, it should be able to require these terms be included. Unfortunately, providers can be at a disadvantage in bargaining power with the IT service provider. In these situations, the health care provider should focus on the most important HIPAA-related elements of the transaction, including protection of PHI, breach response, and access to data both during and upon termination of the agreement. To the extent applicable state law is more restrictive than HIPAA, state law requirements should be included in the BAA.

Excluded Personnel. The IT vendor should represent and warrant that neither the company nor any of its principals, employees, or agents have been excluded from participation in any federal health care program and that the vendor will regularly monitor (i.e., on a monthly basis) HHS's exclusion database to confirm continued compliance.

Health Care Liability and Indemnity Provisions. Most vendors seek to limit liability exposure to the cost of the contract. Because health care is a highly regulated industry, standard indemnity provisions may not cover the risks posed by regulatory enforcement actions including investigations, penalties, and lost income arising from failure to follow Medicare or other payer rules. Also, the liability exposure associated with a potential IT failure, both to patients and cash flow can be catastrophic. The attorneys negotiating the contract on behalf of the health care provider should therefore include language in accordance with state law to make sure the provider is protected from these losses when caused by the conduct of the vendor.

Author Profiles

MICHAEL D. RECHTIN is the chair of Seyfarth Shaw's Data Center Services group and a co-chair of the Commercial Contracts & Outsourcing Transactions group. Mike works at the intersection of real estate, technology and outsourcing. Clients turn to him as one of the very few recognized legal experts in data centers, backed by almost three decades of experience in real estate law. Mike is innately aware of the nuances and intricacies of data centers and is unafraid to get his hands dirty with the technical side of data centers and their related documentation. This natural comfort with data centers, their technical nature, and unorthodox contracting led to Mike further penetrating the IT contracting realm. Mike has represented many health care providers, enterprise companies, financial institutions, high-tech companies, and data center developers/providers in the data center and IT space, and has negotiated transactions ranging from small colocation hosting agreements to complete outsourcing of a client's IT infrastructure stack to several vendors. Contact him via email at mrechtin@seyfarth.com.

CHRIS DEMEO is a partner in Seyfarth Shaw's Health Care group. Hospitals, physician groups, pharmacies, post-acute providers, and independent diagnostic facilities turn to Chris for guidance on a number of matters. His clients must comply with state and federal health care statutes and regulations regarding fraud and abuse, patient information privacy, licensing, and reimbursement. They must structure legally compliant business transactions in the health care sector. In some instances, they also face litigation from state and federal governments, business associates and competitors, and patients. To serve his clients, Chris draws upon his unique perspective, qualifications, and experience. His extensive work in litigation, compliance, and transactions allows him to advise clients from a multifaceted perspective. Additionally, Chris's experience working as an in-house attorney allows him to see matters from his clients' perspective. Contact him via email at cdemeo@seyfarth.com.

AMY S. LEVIN is a partner in Seyfarth Shaw's International Department and a member of the Firm's Data Center Services group. Her practice is focused on domestic and international commercial transactions for multinational companies. Corporate clients turn to Amy for assistance with a variety of complex commercial transactions, including cross-border outsourcing and tech transactions, global licensing and distribution transactions, sourcing and supply chain transactions, commercial contracts, and other corporate and commercial transactions. She is also uniquely qualified to manage large, multijurisdictional transactions for global clients, including global IP transactions, global licensing and distribution arrangements, global risk assessments, reorganizations and post-acquisition integrations, and long-term supply arrangements. Contact her via email at alevin@seyfarth.com.

SHERYL T. DACSO is a partner in Seyfarth Shaw's Health Care group. She concentrates her practice on health care compliance, regulations, and transactions, including physician practice mergers, acquisitions, and business ventures as well as digital health and telemedicine. Her practice includes the representation of nonprofit organizations such as Federally Qualified Health Centers, Certified Nonprofit Health Corporations, medical education foundations, and research organizations. She often advises on joint ventures involving exempt and nonexempt organizations and addresses issues associated with governance and regulatory compliance. Sheryl is a thought leader and frequent speaker on many health care topics, such as health information technology—including digital and e-health transactions, HIPAA and privacy, and Telemedicine use and regulation—as well as health care reform, Accountable Care Organizations (ACO), health information exchanges, and the various rules and incentives associated with the use of electronic health records. Contact her via email at sdacso@seyfarth.com.

AMERICAN
HEALTH LAW
ASSOCIATION

1099 14th Street, NW, Suite 925 • Washington, DC 20005
(202) 833-1100 • Fax (202) 833-1105 • www.americanhealthlaw.org