McKnight's
Long-Term Care News & Assisted Living

Andrea Lee

March 12, 2018

Coming to terms with Software as a Service agreements for long-term care

Andrea Lee

According to a 2017 survey, nearly 88% of healthcare organizations use Software as a Service (SaaS) products.[1] Thus, most long-term care providers are familiar with SaaS agreements, even if they do not recognize them by name.

For instance, long-term care providers typically enter into SaaS agreements when implementing electronic medical records software or when contracting for certain human resources and payroll functions. SaaS arrangements are distinguishable from traditional software licensing arrangements because the software is made available through a website, rather than being installed on the provider's computer system. SaaS providers charge service fees on a recurring periodic basis, instead of charging a large upfront fee.

Like most traditional software licensing agreements, SaaS agreements are generally written with the software provider's — not the customer's — best interests in mind. And depending upon the size of the organization, it may be difficult to negotiate the SaaS provider's terms. Smaller long-term care providers may have the bargaining power only to negotiate the contract duration, while larger providers typically engage in the extensive negotiation of risk allocation provisions, such as limitation of liability, indemnification, and service standards.

No matter where your organization falls on this size spectrum, all long-term care providers should understand the following key terms in their SaaS agreements. Each of these key terms can present significant risks if not negotiated or, at a minimum, understood.

• ***HIPAA***. When a nursing home enters into a SaaS agreement, it is imperative to consider whether the SaaS provider has access to residents' protected health information, and is, therefore, a "business associate" under the Health Insurance Portability and Accountability Act, commonly known as HIPAA.[2]

If the SaaS provider is a business associate, HIPAA requires the parties to enter into a HIPAA compliant business associate agreement.[3] HIPAA also requires the long-term care provider to consider the arrangement in its periodic risk assessments.[4] Failing to do so (or relying on a SaaS provider's incorrect claims that it is not a business associate) could be a costly mistake.

See, for example, No Business Associate Agreement? $31K Mistake – April 20, 2017.[5] If a SaaS provider is a business associate, ideally the nursing home will add its business associate agreement template as an exhibit to the SaaS agreement. Alternatively, the nursing home should review the business associate agreement proposed by the SaaS provider. The business associate agreement must include the legally required provisions described in 45 CFR 164.504(e) and require the SaaS provider to indemnify the nursing home in the event of a breach.

• ***Fee Increases.*** Although negotiating a fair and reasonable upfront fee is of paramount importance, organizations cannot negotiate a good price and treat the remainder of the contract as an afterthought. SaaS agreements commonly describe how fees are subject to yearly increases on auto renewal or upon notice. Fee increases should be considered in conjunction with the agreement's termination rights and should be eliminated or capped (e.g., to no more than 1% of the preceding year's price).

• ***Termination and Transition***. A SaaS agreement should allow a long-term care provider the ability to terminate the agreement upon reasonable notice without cause and without penalty. The ability to terminate without cause gives the long-term care provider flexibility to terminate in the event the contract is no longer advantageous or superior software becomes available. Long-term care providers should also ensure that the SaaS provider is required to provide it ample notice before it may terminate the contract. The notice time must be sufficient for the long-term care provider to not only find, but also transition its employees and data to, the successor software provider.

• ***Service Level Commitments***. Typically, SaaS agreements will include “availability” or “uptime” guarantees that define when the software will be available (e.g., 99.999%, 99.99%, or 99.95%). If availability of the software is critical (e.g., electronic medical records software), the long-term care provider should seek a higher uptime availability. For less critical services, a lower percentage of uptime may be acceptable. The SaaS provider's failure to meet these uptime guarantees should result in corresponding fee credits detailed in the agreement (commonly referred to as “service level credits”) and be a cause for termination or other remedies.

• ***Click-Wrap or Browse-Wrap Agreements***. Long-term care providers should carefully protect any special terms they have negotiated from being overridden by click-wrap or browse-wrap agreements that users must accept before using the software. All technology users are familiar with the “click-to-agree” terms and conditions that they must accept before they can use software or an app.

These click-wrap agreements may contain terms (such as governing law, indemnity, and arbitration provisions) that conflict with the SaaS agreement. Accordingly, long-term care providers should request the addition of a clause to the SaaS agreement stating that the agreement supersedes any default click-wrap or browse-wrap agreements that users are required to accept.

Although the terms above are common, SaaS agreements vary between vendors and each will have unique risks, depending upon the parties and circumstances involved. Thus, while this article provides general guidelines, it cannot be used as a definitive source to answer all legal or business questions about a specific SaaS agreement. Long-term care providers should consider engaging a qualified healthcare attorney to answer their specific questions about SaaS agreements.

[1] HIMSS Analytics, 2017 Essentials Brief: Cloud, http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiz78alxunYAhVRS6wKHRjUDcYQFggsMAA&url=http%3A%2F%2Fwww.himssanalytics.org%2Fsites%2Fhimssanalytics%2Ffiles%2FCloud%2520Study_2017%2520Snapshot.pdf&usg=AOvVaw2lEFQThuZrsiQoYCYW_k-o (last visited February 15, 2018)

[2] Guidance on HIPAA & Cloud Computing, Department of Health and Human Services (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html.

[3] 45 CFR 164.504(e).

[4] 45 CFR 164.308(a)(1)(ii)(A). See also, $750,000 HIPAA Settlement Underscores the Need for Organization Wide Risk Analysis, Department of Health and Human Services (December 14, 2015), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/university-of-washington-medicine/index.html.

[5] Id. See also, Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million, Department of Health and Human Services (August 4, 2016), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ahcn/index.html.

Andrea Lee (@AndreaLeeAtt) is a healthcare attorney at Honigman Miller Schwartz and Cohn LLP.

DISCLAIMER: The views expressed in this article are my own and do not represent those of my employer. This article was created for informational purposes only, does not constitute legal advice and does not create an attorney-client relationship.