Cybersecurity in CTAs: Why Sponsors Need to Get Ahead of It Now

06-23-21 • alert • katherine leibowitz

Welcome to the new frontier for clinical trial agreements: cybersecurity. While cyber risk itself is not new, cybersecurity language is making its way into clinical trial agreements (CTAs) and rightfully so. Sparked by the massive work-from-home shift occasioned by COVID-19 and high-profile ransomware and other security incidents, research institutions are increasingly asking sponsors to agree to security and data breach obligations in the CTA.

Sometimes CTA cybersecurity obligations apply to the study generally; other times, they address only remote monitoring. In addition, to facilitate remote study monitoring (for source data verification and auditing, not subject visits), some sites present a separate remote monitoring agreement, either as a paper contract signed by the site and the sponsor or as a clickwrap agreement/end user license agreement "signed" (by clicking "I agree") by the study monitor. A discussion of remote monitoring agreements is beyond the scope of this post [1].

Based on the CTA cybersecurity language that we are seeing, the impact of the provisions will span much of the clinical trials contracting process because the sponsor's downstream vendor and consulting agreements will likely need flow-down terms.

Whenever a new concept makes its way into CTAs, it takes time for standardized language to develop across the industry. Because cybersecurity language is a newcomer to CTAs (other than for a small minority of research institutions that have included it for several years), standardized CTA language does not currently exist. Some sponsors have not received any cybersecurity language from study sites; other sponsors see it periodically and with increased frequency. While cybersecurity provisions are not yet routinely included in CTAs across study sites, we expect that they will be eventually.

This post explores CTA cybersecurity obligations proposed by study sites and recommends steps for study sponsors to mitigate their risk. Here is what we are seeing.

One-sided obligation of sponsor:

The CTA cybersecurity language proposed by the site is almost always a one-sided obligation of the sponsor, although, in our experience, sites are amenable to negotiating the language and to making at least some of the terms mutual. Cybersecurity language should be mutual, as the risk is mutual. Either party could have a data breach. Further, the electronic touchpoints between the site and the sponsor (often provided via the contract research organization (CRO), such as the electronic data capture (EDC) system) create mutual risk for the introduction of ransomware or other malware into the other party's systems. Some may argue that a one-sided provision is appropriate because, as HIPAA

covered entities, study sites are at greater risk for regulatory violations. But the risk to sponsors is real. Sponsors may have state law obligations and damage control/reputational concerns regarding study subjects, not to mention the potentially severe consequences of ransomware or other malware infecting their electronic systems. Furthermore, public company sponsors need to comply with cybersecurity risk and incident disclosure obligations.

Broad scope of data breach:

PHI and PII: Some sites require sponsors to report breaches of protected health information (PHI) and/or personally identifiable information (PII), and they expand the scope to include not only PHI/PII of study subjects, but also of other patients and individuals at the site. This unnecessarily shifts risk onto the sponsor. Sites should have procedures and electronic controls to limit the slice of information they make available to sponsors (specifically, PHI of study subjects that the sponsor has requested access to for the study). Sponsors are accustomed to agreeing that if their monitors are inadvertently exposed to PHI of patients (i.e. non-study subjects) while on site, the monitors will keep that PHI confidential. However, when it comes to remote access of electronic systems, sites that are unable to limit monitor access to the specific slice of PHI that the sponsor requests access to are creating extra cyber risk for themselves and for their subjects and patients. The burden of that risk belongs to the site. Sponsors should not take on responsibility for a site's systemic "oversharing" of PHI or PII.

Confidential Information: Some sites make the CTA confidentiality obligation mutual and require the sponsor to notify them of any unauthorized access, use or disclosure of the site's confidential information. Often, the definition of site confidential information is quite broad and exposes the sponsor to excessive risk and administrative obligations.

Notification of actual or suspected data breach or security incident:

Some sites ask sponsors to report "actual or suspected" data breaches or security incidents (here, we use the term "breach" to cover both). Sponsors may find it both daunting and administratively burdensome to report all "suspected" breaches. For this reason, the term "breach" needs to be carefully defined and coordinated with the sponsor's information technology (IT) department. If you are the non-breached party, you want to know ASAP if the other party suspects it has a problem. Quick notice enables you to take steps to minimize the impact on your systems. Further, your insurance carrier likely needs to be notified immediately, so it is prudent for each party to agree to notify the other of actual or suspected breach quickly. A related consideration is what "breach" means. Sometimes the CTA includes vague terms like "inappropriate use" or "improper use" in the section on breach reporting. The terminology bears careful review.

Timing of notice:

The timing for notice of breach varies from CTA to CTA. Examples include immediately, promptly, 5 business days and 10 business days. Sponsors need to involve IT to confirm that they are committing to notice obligations they can meet while keeping in mind that the same notice period should apply if the site has to notify the sponsor of an actual or suspected breach.

Mitigation and cooperation:

Some CTAs require the sponsor to take all steps the site requests "in its sole discretion" to remediate a suspected or actual breach. The language may obligate the sponsor to fully cooperate with the site to investigate potential or actual breaches, and to reimburse the site for all costs associated with the investigation and remediation. The costs of forensic

investigation, breach notification, legal fees, regulatory fines and penalties, not to mention follow up litigation, can quickly reach millions of dollars. Given the shared nature of cyber risk, sponsors should push back and require mutuality. Making the provision mutual (which it should be) would force the parties to compromise and settle on more reasonable terms.

Security measures:

Sites impose a variety of security standards on sponsors, such as:

– sponsor must maintain administrative, physical and technical safeguards (sites are used to this from HIPAA)

– sponsor must encrypt data at rest and in transit (again, the scope of data coverage matters; this may include PHI, PII and/or all confidential information)

– all devices accessing the site's systems must have up-to-date anti-virus/anti-malware software

– requirements around using site Wi-Fi (if permitted, site may provide endpoint protection software for monitor's machine) or public Wi-Fi (prohibited; use is at sponsor's sole risk).

Compliance with HIPAA:

Some CTAs require sponsors to comply with HIPAA even if the sponsor is not a HIPAA covered entity (most sponsors are not; further, sponsoring a clinical trial does not make the sponsor a HIPAA business associate). Most lawyers believe this is not prudent, as agreeing to comply with HIPAA puts the sponsor in immediate breach of the CTA if the sponsor is not HIPAA compliant (becoming and remaining HIPAA compliant is time consuming, resource intensive and expensive) and could theoretically expose sponsors to significant fines and penalties for HIPAA violations. That said, at a recent MAGI clinical research conference panel on cybersecurity, we polled the audience and found that 72% of sites require sponsors to comply with HIPAA, and, surprisingly, 69% of sponsors and service providers agree to comply with HIPAA even though they are not HIPAA covered entities. That said, we consider it best practices not to agree to comply with HIPAA if you are not a HIPAA compliant entity. We recommend that the CTA clarify that the sponsor is not subject to HIPAA and that it will comply with laws and regulations applicable to sponsor.

Use and disclosure of PHI only pursuant to the informed consent, HIPAA authorization and applicable law:

This language is not new and is a reasonable requirement, but sponsors need to look at the wording carefully to see if the terms require them to impose obligations on their downstream contractors.

Responsibility for employees, agents and contractors:

In terms of downstream vendor contracts, this is where it can get quite tricky for sponsors. Some site CTAs require sponsors to have written agreements with their employees, agents and contractors, including CROs, consultants and all other downstream vendors (let's call these the sponsor's team), obligating them to comply with the CTA's cybersecurity obligations. Importantly, many sites make the sponsor liable for any losses or damages caused by the sponsor's team. Sponsors often already have their downstream services agreements in place, and those agreements likely do not address cybersecurity to the degree that the CTA requires. This means the sponsor needs to review and possibly amend those agreements, depending on the CTA language and the sponsor's risk tolerance.

Indemnification and Limitation of Liability:

Indemnification:

– The impact of the wording of the indemnification section can be very subtle. For example, the sponsor may unwittingly be indemnifying the site for losses due to a security breach if, for example, the sponsor's indemnity broadly covers losses arising from or relating to the study. At the other end of the spectrum, the sponsor may specifically indemnify the site for security breaches that the sponsor causes. Somewhere in the middle in terms of subtlety is sponsor indemnification for breach of its obligations in the CTA. Whether or not this would cover security breaches would depend on the sponsor's obligations in the CTA, such as provisions relating to cybersecurity, confidentiality and PHI. Indemnification for negligence could also lead to sponsor coverage of security breach costs.

– Sponsors have a lot to juggle when considering indemnification obligations related to cybersecurity. Sponsors should require reciprocal indemnification by the site. Sometimes, this is not possible, particularly for certain public universities that are prohibited by state law from indemnifying. Either way, sponsors should carefully review the indemnification language and accompanying carveouts to mitigate their risk. In addition, sites are increasingly asking sponsors to indemnify for losses caused by the sponsor's team, including CROs and other contractors. Furthermore, sponsors need to ensure that their downstream vendor agreements have appropriate backup indemnification.

Limitation of Liability: No indemnification provision is complete without a review of the limitation of liability section (i.e., mutual exclusion of consequential damages and liability cap). The CTA parties are accustomed to viewing these provisions through the lens of subject injury, and eventually, it may become standard to take into account cybersecurity. Business Associate Agreements, web hosting agreements, software as a service (SaaS) and other technology services agreements often cap certain indemnification obligations and clarify whether and how the limitation of liability language relates to the indemnification section (e.g., whether a certain type of loss is direct), particularly in the cybersecurity context. While these can be useful tools to mitigate risk, we expect it will take a little longer for these concepts to make their way into CTAs.

Insurance:

A small number of sites insert one-sided (on the sponsor) cyber insurance obligations into the CTA. Having appropriate cyber insurance is critical. This provision should be mutual if the sponsor maintains cyber insurance (many do not). Those who do not have cyber insurance should obtain it. The ins and outs of cyber insurance are too numerous to address here. It is important to understand your policy coverage and, at a minimum, to see the other side's certificate of insurance.

Downstream Vendor Agreements:

Based on what we are currently seeing in CTAs and our expectation that standardized terms will develop due to both enhanced awareness of cyber risk and the enactment of state privacy and security laws (e.g. California and Virginia both take a GDPR-like approach), we recommend that sponsors audit their downstream agreements to ensure they have appropriate language to address cybersecurity risk. This post provides a roadmap for the sections to consider, and we expect that these topics will evolve over time. Sponsors who have not already done so will need to do a data mapping exercise for their study data. While the most obvious data that come to mind are PHI and PII, the mapping process should

cover all study data and any confidential information from the study sites. Different levels of risk will apply to the different data types. Among other things, sponsors need to know where their data is going, how it gets there and who provides the technology. Some obvious vendors include: CRO services, EDC development and hosting, risk-based monitoring, statistical analysis, safety committees (e.g. DMC and CEC), medical monitors, consultants, software as a service (SaaS), and other contractors and technology vendors. Going forward, sponsors should have standard language to add to their new vendor agreements (but properly tailored to the vendor), as it is administratively much easier to address this proactively rather than to have to go back and renegotiate the downstream agreements.

Recommendations:

With the use of electronic data capture (EDC) systems and other technologies, Sponsors, sites, CROs, EDC vendors and others in the services and communications chain serve as touchpoints where security breaches can be introduced. Cyber risk is real and is shared. We recommend that sponsors:

(a) pay close attention to the nuances of CTA cybersecurity language proposed by study sites and its interaction with other provisions of the CTA;

(b) work with legal and IT to develop a mutual CTA cybersecurity provision that is consistent with their existing internal practices and personnel obligations and that is supported by downstream obligations in their vendor agreements. Sponsors that comply with a third-party standard or have a third-party certification should start there when drafting language (e.g. ISO/IEC 27001, NIST, CCPA/CPRA, SOC 2, etc.). Because of the shared risk, sponsors should consider including cybersecurity provisions proactively in their CTAs. At a minimum, sponsors should have a provision or policy in hand to respond to language proposed by the sites;

(c) confirm that the CTA language is consistent with their internal practices and personnel obligations;

(d) confirm that their downstream vendor agreements have flow-down and backup language and amend those agreements if necessary; and

(e) proactively include cybersecurity language in new vendor agreements while keeping in mind what sites are requiring in CTAs. Again, sponsors should work with legal and IT to develop standard language.

Sponsors should prepare now for their CTAs and vendor agreements to address cybersecurity. This is best practices and protects the parties as well as study subjects. Sponsors can and should help steer the development of industry standard CTA cybersecurity language. It is in the interest of all parties to come up with mutually agreeable language. Security breaches will not wait, nor should your contracts.

The above recommendations represent our current thinking and will likely evolve as industry standards develop and technology changes. We can help you evaluate your CTAs and vendor agreements for cyber risk and craft and negotiate appropriate language. We will continue to monitor this space and encourage you to check our News & Insights for updates.

[1] The remote monitoring agreements we are seeing tend to be substantially more onerous than the CTA security language we explore in this post. Remote monitoring agreements often include unfeasible obligations, language that undermines the CTA's indemnification and limitation of liability provisions and other surprises for sponsors.

If you have any questions or would like more information about these developing issues, please contact the following:

KATHERINE LEIBOWITZ
1-610-896-5788
Katherine.Leibowitz@LeibowitzLawTeam.com