China: Data Protection Statement

OneStudyTeam provides a cloud-based clinical trial platform, *StudyTeam*, that helps clinical research sites with patient enrollment and management. In so doing, OneStudyTeam is committed to protecting the privacy, integrity, and security of those who entrust us with their personal, clinical, or health data that we may process in all aspects of our business worldwide. At OneStudyTeam, we aim to provide a compliant and consistent approach to data protection through the establishment of a robust and effective data protection program that complies with existing laws and abides by data protection principles. OneStudyTeam is compliant with the Personal Information Protection Law (PIPL) and the regulatory landscape in China.

What laws and regulations govern China?

Multiple regulations govern StudyTeam operations in China, including: the Population Health Information Regulation, the Big Data Regulation, the Regulation on the Management of Human Genetic Resources, the Detailed Implementation Rules for the Management Regulations of Human Genetic Resources, the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law (PIPL). The regulations form a backdrop for the types of data that can be collected, how they are to be protected and processed, and where the data can be stored.

The Data Protection team at OneStudyTeam actively tracks and monitors the ever-changing regulatory landscape to remain compliant as new regulations are introduced. OneStudyTeam recognizes that the global data protection field can change quickly and we take an active stance toward compliance.

What makes it safe and compliant for sites to enter patient data in a Software as a Service (SAAS) product like *StudyTeam*?

Privacy by Design: In choosing to partner with OneStudyTeam, a site, as the Data Controller (referred to as "Data Handler" in PIPL), has a broad range of options in determining what data to enter into *StudyTeam*, an application that has incorporated data protection into the software from the ground up.

StudyTeam has integrated appropriate technical, contractual, and organizational safeguards to ensure compliance with data protection principles such as data minimization, accountability, integrity, and confidentiality. The software is also abundantly flexible to ensure that Data Controllers, such as clinical trial sites, are truly in control over what data goes into the software, where it is transferred, and for how long it is retained.

Moreover, *StudyTeam* features hard-coded protections against human error. *StudyTeam* locks—without possibility of override—data fields known or likely to contain identifying patient information, thus prohibiting those fields from being replicated outside of the site's

particular instance of *StudyTeam*. Built-in protections like these allow sites to eliminate their risk of inadvertent disclosure of sensitive patient information.

OneStudyTeam has established robust technical and organizational measures (TOMs) appropriate to the nature of the data and processing activity. Our TOMs include appropriate policies defining data classification, encryption, data retention, and incident response.

In addition to robust technical controls, OneStudyTeam protects patient data through organizational and administrative measures designed to ensure that patient data is processed only to the extent necessary and by those who have a need to know. For example, OneStudyTeam requires all data sub-processors to undergo a privacy, security, and legal review and approval process prior to being accepted as a vendor to OneStudyTeam. As part of the contracting process, OneStudyTeam requires vendors to sign relevant data protection terms (for example, a data protection agreement and/or data transfer agreement) to ensure that OneStudyTeam's commitments to protect patient data are also reflected in our vendor contracts. OneStudyTeam also conducts regular data protection training across our entire workforce and provides additional role-based privacy training as appropriate.

Does OneStudyTeam participate in Ethics Committee Reviews?

StudyTeam for Sites supports site staff in their management of patient pre-screening and enrollment information; it is not patient-facing and it is not intended to store clinical source documents. As such, *StudyTeam for Sites* is generally not subject to Ethics Committee review. However, each site follows their own policies and procedures to determine what regulatory authorities need to be informed about their use of OneStudyTeam.

StudyTeam eSource, on the other hand, stores source documentation and may be subject to Ethics Committee Review.

In any event, if a site elects to seek Ethics Committee review, OneStudyTeam will provide all information required by the site in support of its submission.

How often is OneStudyTeam audited?

In addition to conducting our own internal audits of our systems, OneStudyTeam is regularly audited by Sponsors. Each Sponsor has their own timeline for conducting audits of their vendors, but OneStudyTeam actively complies and participates in those audits in accordance with the Sponsor's requirements. Additionally, OneStudyTeam is audited annually to maintain ISO 27001 compliance.

What security certifications can OneStudyTeam share?

OneStudyTeam has an ISO 27001 Certificate that can be shared upon request.

Does OneStudyTeam have a Data Protection Officer (DPO)?

OneStudyTeam's Global Data Protection Officer (DPO) leads OneStudyTeam's privacy program, which focuses on monitoring and addressing privacy risks across all business units and practices. From its conception, OneStudyTeam's privacy program adheres to the principles of privacy-by-design and privacy-by-default in all aspects of its products and services, and under the purview of the DPO, OneStudyTeam's privacy program effectively protects personal data at each point of the data life cycle.

How does OneStudyTeam utilize contractual protections to comply with the PIPL and other Chinese regulations?

OneStudyTeam's software terms, the PIPL Standard Contractual Clauses (SCC), and our Data Protection Agreement (DPA), outline our privacy policy and how our cloud-based system is built atop a technology stack dedicated to storing and managing personal data. Similar to the EU General Data Protection Regulation (GDPR) SCCs, the PIPL SCCs can be used for outbound transfer of personal information that does not need to undergo a security assessment under China's PIPL. However, other regulations within China may require the site and/or OneStudyTeam to conduct assessments and/or register with an agency. Ultimately, the site will determine what assessments and/or filings are necessary.

The software terms and the DPA are designed to work in tandem to ensure that the rights and obligations of each party concerning the protection of personal data are clearly defined, including the subject matter and duration of the processing, the nature and purpose of the processing, the administrative and technical safeguards in place, and the type and category of personal data involved. Notably, the Data Protection Agreement ensures that data entered into *StudyTeam* is and remains within a site's control and direction.

Who is responsible for site data?

Data Controller

OneStudyTeam is the Data Processor ("entrusted party") and the site is the Data Controller or Data Handler.

As the Data Controller, each site independently determines the purpose and means for which data is collected and how it is shared. Each site determines that any data they instruct OneStudyTeam to transfer is within their rights to authorize and is a lawful transfer.

As the Data Processor, OneStudyTeam will process the data in strict accordance with the instructions of the site.

Site-Sponsor Separation

StudyTeam for Sites and *StudyTeam for Sponsors* are two separate and distinct platforms, with the option of interconnectivity (at the site's option). Sponsor users do not have access

to the site platform, and site users do not have access to the sponsor platform. Only if a site elects to "connect" a particular trial to the relevant sponsor, *StudyTeam for Sites* will transmit limited de-identified reporting information to the sponsor, eliminating the need for the site to send a separate enrollment report to the sponsor.

OneStudyTeam typically licenses *StudyTeam for Sites* directly to sites. This is done through an agreement called the *StudyTeam for Sites* Terms of Service. The Terms of Service include a regionally appropriate Data Protection Agreement (DPA) and, if relevant, Standard Contractual Clauses (SCCs) addressing how the site and OneStudyTeam will work together to ensure that the site's data is protected appropriately and according to applicable privacy laws. Importantly, these data protection terms establish sites as the Data Controller of personal data that is processed within that site's individual instance of StudyTeam.

So long as the site has signed the *StudyTeam for Sites* Terms of Service, sites are free to use *StudyTeam* to manage their enrollment data for any trial, with or without ever connecting their data to a Sponsor. In other words, so long as the site has signed the Terms of Service, a site does not operate under a license from a Sponsor.

Data Scope and Control

As the Data Controller, each site determines the purpose for which data is collected and how it is shared. Sites have a broad range of options in determining what data to enter into StudyTeam. StudyTeam can be used in a de-identified manner; i.e., StudyTeam can be configured in such a way that no identifying patient information is entered at all. However, most sites find it useful to enter at least some patient identifying details. Notably, StudyTeam does not store patient medical records; it stores data to facilitate the pre-screening process.

If a site chooses to send reporting data to a designated trial Sponsor, *StudyTeam* includes controls designed to ensure that data associated with a particular trial is only shared with the appropriate Sponsor. The Site-to-Sponsor connection is enabled by OneStudyTeam on a per-trial basis and only after receiving affirmative instruction from the site. Moreover, the site remains in full control over what data points are shared with a Sponsor. For example, though a Sponsor may request a particular set of data points as part of the pre-screening/enrollment reporting, the site ultimately decides what is or is not included in that report. As an added layer of protection, data fields that are known to be identifiable (*e.g.*, patient name) are protected in a hard-coded manner so that even if a Sponsor were to request, and a site were to approve, the transfer of that identifiable data, the software will simply not be able to fulfill that request.

Which types of data subjects have their personal data stored or processed by OneStudyTeam based on Customer (Data Controller) instruction?

- Patients or research subjects of the Customer
- Customer's authorized users of OneStudyTeam's products and services

What categories of personal data are stored or otherwise processed within *StudyTeam for Sites* ("Site Data")?

The types of data may include, but are not limited to:

- Name
- Physical address
- Email address
- Telephone number
- Professional role & affiliation
- Date of birth
- Biometric data
- Gender
- Race
- Ethnicity
- Research indications
- Appointment dates and details
- Data concerning health

What categories of personal data are transferred to *StudyTeam for Sponsors* for purposes of reporting to research sponsor ("Reporting Data")?

The types of data may include, but are not limited to:

- Gender
- Race
- Ethnicity
- Research indications
- Appointment dates and details
- Research site-usernames, contact details, and professional affiliations

Data Storage

Chinese sites' *StudyTeam* data is hosted in AWS-Ningxia, China, ensuring that identifiable patient data remains within the region. Reporting data and staff user information (*e.g.*, email address and username) will be transferred to the United States. To the extent a site chooses to connect a trial to a Sponsor via *StudyTeam*, de-identified reporting information (*e.g.*, information recorded in the pre-screening logs) will also be transmitted to the United States. We take data security seriously and implement appropriate technical and organizational safeguards to protect all data that is shared with the application. (For more information on data security, please refer to the above section "*What makes it safe and compliant for sites to enter patient data in a Software as a Service (SAAS) product like StudyTeam?*" or to OneStudyTeam's Data Privacy & Security page.)

Data Retention

In order to provide flexibility for sites and in recognition that individual sites are subject to differing standards and oversight, sites, as Data Controllers, direct OneStudyTeam on the retention of data. Because different sites can be subject to different retention requirements depending on their jurisdiction and other variables, StudyTeam does not have a predetermined retention period. OneStudyTeam will follow the site's instructions to delete data, subject to applicable law.

What are OneStudyTeam's obligations in terms of data sharing?

Applicable regulations, Data Controller authorization, OneStudyTeam's Privacy Policy, and contractual commitments (for example, Data Protection Agreements and Standard Contractual Clauses), all govern OneStudyTeam's data sharing obligations. With the Data Controller's authorization, OneStudyTeam partners with third parties to enhance our product offerings whereby data may be shared with those third parties called "sub processors." OneStudyTeam maintains a current list of all sub processors here. This list is updated after new sub processors are approved through OneStudyTeam's internal review process. Sites can sign up to receive email notifications prior to the addition of new sub processors by signing up through the form on the subprocessor page.

Further, OneStudyTeam's Data Privacy & Security page lists the minimum criteria for becoming an approved subprocessor. OneStudyTeam requires all third-party vendors, tools, and service providers to undergo a privacy assessment and a data security assessment prior to contract signature. These assessments form a central part of OneStudyTeam's vendor qualification process and allow OneStudyTeam's Data Protection Officer and Security Officer visibility and an opportunity to ensure that each third party meets legal requirements and OneStudyTeam's own robust standards. Third parties are routinely required to execute data protection agreements, data transfer agreements, and contractual data security terms as part of the contracting process.

Can a site share trial protocols with OneStudyTeam for trials that are not sponsor-connected?

StudyTeam for Sites is an internal tool to assist clinical research sites discover, pre-screen, and enroll patients. One feature of *StudyTeam for Sites* is the ability to add Sponsor protocols into the application to help address protocol requirements (*e.g.*, I/E Criteria, Visits etc.). The *StudyTeam for Sites* Terms of Service contain strong confidentiality language and, from the OneStudyTeam perspective, any protocol that a site provides remains the site's confidential data and is subject to the confidentiality clauses as well as the Technical and Organization Measures (TOMs) that are in place at OneStudyTeam.

Protocols, in many cases, are publicly available (*e.g.*, via Prospero, AllTrials, or clinicaltrials.gov). There are growing trends for public availability of study protocols to help facilitate detailed assessments of the internal validity of a trial, deter selective reporting of outcomes and analyses, and improve understanding of external validity. Public access to

study protocols is fundamental to the societal value of clinical trials. In the situation where a trial has a publically available protocol, sites can share that protocol with OneStudyTeam to add feature functionality to their *StudyTeam for Sites* instance.

In OneStudyTeam's experience, most Sponsors are amenable to sharing non-publicly available protocols with site-partners who help effectuate clinical trials. Sponsors expect sites to utilize their internal tools in conjunction with documentation provided by the Sponsor to carry-out the trial enrollment efforts.

Sites may also seek the explicit approval to add a protocol into *StudyTeam for Sites* by contacting their sponsor contact.

What if I have more questions about data protection or security?

OneStudyTeam has dedicated resources to help answer any questions you may have. Whether your questions come with initial onboarding, trial setup, ongoing use of our services, or trial closeout, we are here to help. Our Compliance, Legal, Security, and Customer Success teams can help address any questions you may have.

For more information, please visit OneStudyTeam's Data Privacy & Security page or contact your Customer Success representative.

Last Updated: August 2023