StudyTeam Security Overview

StudyTeam Security Overview

Your access to, and use of, any Site or Service is subject to the Terms of Service of Reify Health, Inc., on behalf of itself and its subsidiaries and affiliates (collectively, “Reify”, “we”, “us”, or “our”). This Security Overview (“Security Overview”) is incorporated into and made part of our Terms of Service. All capitalized terms used but not defined herein have the meanings given to them in our Terms of Service.

Reify Health, Inc.’s online products and services (collectively, the “Services”) available through its web sites https://studytem.reifyhealth.com and mobile applications (collectively, the “Sites”, and each, a “Site”) consist of a technology platform that allows Registered Users to use the Sites to identify, evaluate, and procure clinical research services from clinical investigators and their staff and institutions during clinical research activities (“Third Party Providers”) and to observe the performance by such Third Party Providers of such clinical research services. Reify Health applies industry standard security practices and manages platform security so Registered Users can focus on conducting research. Our platform is designed to protect Registered Users from threats by applying industry-standard security controls at every layer from physical to application.

System Security

Registered Users access Reify Health’s Sites through a secure web portal. All data are protected with SSL encryption during transmission. The web application is hosted on a separate application server. All servers can only be accessed using key-based authentication, and we employ access control policies to secure appropriate access and to ensure that all data are protected. We employ a rigorous data backup protocol.

Data Confidentiality and Retention

During the course of operating the service, Reify Health collects and stores Registered User information that falls into the categories outlined in the Terms of Service. Reify Health protects these forms of Registered User data by maintaining strict isolation between the production environment and the development environments. Security policies are applied to ensure Reify’s access to Registered User data is restricted to employees with a legitimate business need. We perform regular backups of customer data.

We may store and use your Personal Information for as long as you continue to access or use any Site or Service and thereafter in accordance with our Privacy Policy. Reify Health will retain your Personal Information indefinitely for the purposes of audits and review in the course of providing the Services and for the substantiation of other data in the system.

Upon identification of any unauthorized PHI entering our system, Reify will a) inform the sender of unauthorized receipt, b) destroy any copies of the PHI or consult the Reify Information Officer in the event destruction is not possible, and c) document that PHI has been redacted from our system.

Reify Health currently utilizes an enterprise-level third-party provider to deliver our services, and some Registered User data are subject to the security policies of these providers. Reify Health operates its

services in Aptible, a cloud-based infrastructure provider that provides its own security, availability, reliability, redundancy, and performance commitments. For details, see Aptible's latest security policies, terms of service, and privacy policies. We will provide Customers with a copy of these policies upon request. We reserve the right to add and/or substitute third-party providers, at our sole discretion.

We may update this Security Overview over time. When we do, we will also revise the "last modified" date at the bottom of this document. For material changes to this data security policy, we will notify you by placing a notice on the home page of Reify Health or by sending you a notification directly.

Last modified: 16 May 2016