User Privacy Policy

The language provided below is displayed for the user within the application.

Purpose

This Privacy Policy describes how snapIoT addresses regulatory requirements related to Personally Identifiable Information, Personal Health Information, Patient Privacy, the EU General Data Protection Regulation (EU GDPR), the California Consumer Protection Act (CCPA) and other applicable privacy laws and regulations.

Scope

This Privacy Policy describes how snapIoT collects, uses, discloses, and otherwise processes personal information in connection with our websites, mobile apps, and other services, and explains the rights and choices available to individuals with respect to their information.

Data Collected by snapIoT

snapIoT is a provider of software and services to life sciences companies for use in the conduct of clinical trials throughout the world. Acting as a third-party agent for our clients, snapIoT receives and processes Personal Data (name, email, phone number) from study sponsors, research site staff, various consultants/subcontractors, and employees.

Additionally, as specifically authorized by our customers, snapIoT may also collect and store clinical study data, which is collected according to a project-specific informed consent with clinical research subjects, and may include detailed information regarding health status, medical assessments, test results, and other data required for a particular study.

snapIoT intends that its corporate privacy policies, internal SOPs, and work practices are adequate to ensure compliance with applicable international laws and regulations including the European Union's General Data Protection Regulation (GDPR) and the California Consumer Protection Act (CCPA). Detailed contractual arrangements, Standard Contractual Clauses, SOPs and business policies govern all work with customer data and are available for audit/review by clients and regulatory authorities.

Dispute Resolution

snapIoT is committed to resolving complaints about privacy and the collection or use of personal information. Individuals with inquiries or complaints regarding the Privacy Policy should first contact snapIoT at DPO@Labcorp.com or the mailing address below:

snapIoT

Privacy Office, LabCorp, 531 South Spring Street, Burlington, NC 27215

General Data Protection Regulation (GDPR)

This regulation is directly applicable to each member state of the European Union and affects data controllers and processors inside and outside of the EU which collect data on EU data subjects.

snapIoT assessed its technical and procedural safeguards to ensure compliance with the GDPR which are outlined below.

GDPR Definitions

For purposes of this regulation, the following definitions apply:

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'processing' means any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

'third party' means a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

Data Subject Rights

Individuals located in the European Economic Area only, whose Personal Data snapIoT processes ("Data Subjects"), have the following rights with regard to their Personal Data:

Right of access

Data Subjects may request details of their Personal Information that the organization holds. snapIoT will confirm whether it is processing the individual's Personal Information and will disclose supplementary information including the categories of Personal Information, the sources from which it originated, the purpose and legal basis for the processing, the expected retention period, and the safeguards regarding Personal Information transfers to non-EEA countries, subject to the limitations set out in applicable statutes, regulations and other laws.

Right of correction

snapIoT will comply with a Data Subject's request to edit and update incorrect Personal Information promptly. In the event that correction is not possible or cannot occur in a timely manner, snapIoT will document its reasons, specify the time frame in which correction will occur (to the extent knowable), and respond to the requestor with this information within 30 days from the receipt of request for correction.

Right to be forgotten

At a Data Subject's request, snapIoT will delete their Personal Information promptly if:

- it is no longer necessary to retain the Personal Information;
- the Data Subject withdraws the consent which formed the basis of the Personal Information processing;
- the Data Subject objects to the processing of their Personal Information and there are no overriding legitimate grounds for such processing;
- the Personal Information was processed illegally; or,
- the Personal Information must be deleted for snapIoT to comply with its legal obligations.

snapIoT will inform any third parties with whom it might have shared the Data Subject's Personal Information of the deletion request.

snapIoT may decline a Data Subject's request for deletion if processing of their Personal Information is necessary:

- to comply with a legal obligation;
- in pursuit of a legal action;
- to detect and monitor fraud; or,
- for the performance of a task in the public interest.

Right to restrict processing of Personal Information

At a Data Subject's request, snapIoT will limit the processing of their Personal Information if:

- the Data Subject disputes the accuracy of their Personal Information;
- the Data Subject's Personal Information was processed unlawfully and they request a limitation on processing, rather than the deletion of their Personal Information;
- snapIoT no longer needs to process the Data Subject's Personal Information, but the individual requires their Personal Information in connection with a legal claim; or,
- the Data Subject objects to the processing pending verification as to whether an overriding legitimate ground for such processing exists.

Right to notice related to correction, deletion, and limitation on processing

In so far as it is practicable, snapIoT will notify a Data Subject of any correction, deletion, and/or limitation on processing of their Personal Information.

Right to data portability

At a Data Subject's request, snapIoT will provide them a copy of their Personal Information in a structured, commonly used and machine-readable format, if: (i) the Data Subject provided snapIoT with Personal Information; (ii) the processing of the Data Subject's Personal Information is based on consent or required for the performance of a contract; or, (iii) the processing is carried out by automated means.

Right to object

Where snapIoT processes a Data Subject's Personal Information based upon the lawful basis of legitimate interest, then the individual has the right to object to this processing.

Right not to be subject to decisions based solely on automated processing

Data Subjects will not be subject to decisions with a legal or similarly significant effect (including profiling) that are based solely on the automated processing of their Personal Information, unless snapIoT has received explicit consent or where the automatic processing is necessary for a contract with snapIoT.

Right to withdraw consent

A Data Subject who has provided snapIoT with consent to process their Personal Information has the right to withdraw any consent previously provided to snapIoT at any time. If a Data Subject withdraws their consent, this will not affect the lawfulness of snapIoT's collecting, using and sharing of their Personal Information up to the point in time that consent was withdrawn. Even if a Data Subject withdraws their consent, snapIoT may still use the information that has been anonymized and does not personally identify the Data Subject.

Right to complain to a supervisory authority

If a Data Subject is not satisfied with snapIoT's response, they have the right to complain to or seek advice from a supervisory authority and/or bring a claim against snapIoT in any court of competent jurisdiction. Any person at snapIoT that receives a request from a Data Subject seeking to exercise their rights under GDPR should contact the Privacy Office to assist in the review of and response to the Data Subject's request. Requests will be responded to within 30 days of receipt. Under certain circumstances, snapIoT may inform the requesting Data Subject that additional time is needed to fully comply with the request. Such notification shall occur within 30 days of receipt of the request.

Inquiries can be made by contacting DPO@Labcorp.com or the mailing address below:

snapIoT

Privacy Office, LabCorp, 531 South Spring Street, Burlington, NC 27215

Data Protection Impact Assessment

To enhance compliance with the GDPR, snapIoT carried out a data protection impact assessment to help determine the level of protection that is required.

The impact assessment includes the measures, safeguards and mechanisms that mitigate the risk to the data collected and ensures the protection of personal data.

Lastly, it also utilized by snapIoT to demonstrate compliance with the GDPR to the supervisory authorities.

Roles of the Data Controller and Data Processor

In studies that involve Labcorp Drug Development as the contract research organization (CRO), snapIoT is the data controller – as snapIoT is part of Labcorp.

In studies that include a contract research organization (CRO) that is not part of Labcorp, snapIoT assumes the role of the data processor. These relationships are contractually defined between the research organization, study sponsor, and snapIoT.

In all cases, snapIoT maintains compliance to ensure it meets its data protection obligations.

Data Processor Subcontractors

Subcontractors of snapIoT are also subject to the same requirements under the GDPR and they are also bound by any contracts with the controller.

What mechanism does snapIoT use for transfer of data from the EU to the U.S.?

Depending on the study configuration, snapIoT may transfer the data collected to study databases outside of the EU. In this case, snapIoT will enter into the Standard Contractual Clauses, which are EU Commission-approved contracts between data exporters within the EU and data importers in so-called “third countries,” to transfer personal data from within the EU to recipients in those third countries in accordance with GDPR.

How does snapIoT maintain compliance with GDPR?

snapIoT’s standard Data Processing Addendum incorporates the Standard Contractual Clauses (SCCs) for any transfers of personal data from within the EU to the U.S. that occur in connection with snapIoT’s performance of its services. Thus, snapIoT will ensure all new contracts (renewals and new customers) include the SCCs.

- For any existing customers, whose current agreements do not already include the DPA and SCCs, snapIoT can agree to amend the agreement to incorporate both.

- By executing its DPA and the SCCs, snapIoT becomes legally obligated to comply with the relevant requirements of GDPR that apply to snapIoT's performance of its services. To that end, snapIoT maintains robust internal policies and procedures to ensure data security, integrity, and data privacy.
- All data collected by snapIoT on behalf of its customers is collected in accordance with an approved clinical research protocol and a study-specific informed consent obtained from the patient.
- All data is encrypted (256-bit AES) in transit from collection devices to snapIoT's databases and is maintained in pseudonymized form within snapIoT's systems.

California Consumer Privacy Act (CCPA)

To the extent applicable, snapIoT complies with the California Consumer Privacy Act. The Labcorp CCPA privacy policy can be found under www.labcorp.com/california-privacy-policy.