

**At Koneksa Health Inc. (“Koneksa”), protecting Data Subject privacy is part of our commitment to improving health.**

## **THE KONEKSA PLATFORM**

The Koneksa platform is used in support of clinical trials and non-interventional research studies (“Studies”) that are conducted by our clients who are pharmaceutical, biotechnology, and medical device companies, and academic institutions, and others who sponsor research Studies, as well as by individuals enrolled in a Study. We do this by integrating data from wearable devices, mobile devices, apps, and other health devices (collectively, “Devices”) used by individuals who contribute data according to the Study sponsor’s Study protocol, such as yourself or the party for whom you are responsible (“Data Subjects”) who are enrolled within those Studies.

Data is collected by the Devices that are in use by the Data Subject. The data from the Devices is transferred to the Koneksa platform and then sent to the Study sponsor. For purposes of this privacy policy, the Study sponsor is the company who determines the purpose and means of processing personal data (the “Data Controller”) and we are the company who collects data on behalf of, and pursuant to the instructions of, the Data Controller (the “Data Processor”). The exact configuration and Devices the Data Subject may use depends upon the Study in which the Data Subject is being asked to participate. The Study protocol, which is designed and prepared by the Data Controller, defines the Study configuration we are tasked with implementing. The Informed Consent Form (“ICF”), which is also prepared by the Data Controller, and signed by Data Subject with the Data Controller, identifies the Devices being used and the information being collected.

Data Subject privacy is very important to us. By accessing the Koneksa platform or any Device, the Data Subject agrees to the terms of this policy. We may make changes to this policy from time to time that we will post here. The Data Subject’s continued use of the Koneksa platform is deemed to constitute acceptance of these changes, so check back periodically for changes. The Data Controller with whom the Data Subject has engaged is responsible for informing the Data Subject of any substantive changes to this policy, which we will have communicated directly to the Data Controller.

## **CHILDREN UNDER THE AGE OF 18**

The Koneksa platform is not intended for use by children under 18 years of age without the prior consent of a parent or legal guardian. No Data Subject under age 18 should provide any information to or on the Koneksa platform without the prior consent of a parent or legal guardian. We do not knowingly collect personal information from children under 18 without the prior consent of a parent or legal guardian. If the Data Subject is under 18, do not use or provide any information to the Koneksa platform or through any of its features, register on or log into the platform, or provide any information about the Data Subject to us, without the prior consent of a parent or legal guardian. If the Data Subject believes we might have any information from or about a child under 18 without such prior written consent, contact us as noted in the section entitled “How to Ask a Question or Raise a Concern.”

## **DATA COLLECTED BY KONEKSA**

### **WEB BROWSERS**

This section only applies to the Data Subject if he/she has been provided with a login to use the Koneksa web application component of the Koneksa platform. Koneksa does not use third parties to track website behavior or other personally identifiable data elements. Koneksa does however issue its own temporary cookie to users of our web application. The sole purpose of this cookie is to establish and maintain an authorized connection between the Data Subject’s web browser

and our platform. We do not collect any information about the Data Subject through the use of cookies.

## **KONEKSA USER ACCOUNT**

As the Data Processor, Koneksa does not require the Data Subject to provide any personal information to have an authorized user account that will give the Data Subject access to the Koneksa platform or any Device. In some cases, based on the Study protocol as designed by the Data Controller, the Data Subject may receive questionnaires, in which case additional information may be required. Refer to the “Questionnaires” section for details.

## **QUESTIONNAIRES**

If the Study in which the Data Subject is participating requires the person to complete questionnaires on the Koneksa platform, based on the Study protocol design and upon direction from the Data Controller, Koneksa can send the Data Subject reminders via email and/or cell phone.

## **EMAIL**

By default, Koneksa may assign a Study-specific email address (not the Data Subject’s personal email address) that the Data Subject will use for the duration of the Data Subject’s participation in the Study (and which is deleted at the end of the Study). Alternatively, if specifically instructed and agreed upon with the Data Controller, we would allow the Data Subject to use an email address specified by the Data Subject.

## **CELL PHONE**

Koneksa may also send questionnaire reminders as text/SMS messages to the number associated with the cell phone used by the Data Subject. Koneksa will not collect the Data Subject’s cell phone number, unless specifically instructed and agreed upon with the Data Controller.

Automated notifications issued to the Data Subject are sent by the Koneksa platform and not directly by persons engaged by our client or Koneksa. Notifications are generically addressed and do not contain personally identifiable information (“PII”) or information relating to any health condition. Such notifications will not be shared outside our platform. As the Data Processor, we will not contact the Data Subject directly for any purpose other than sending the Data Subject notifications about reminders to complete questionnaires or activities (e.g., assessment schedule notifications) or about the underlying account. Any and all other communications will be issued by either the Data Controller or their representative, such as a Study site coordinator.

When the Data Subject completes a Study or if the Data Subject withdraws consent to continue to participate in the Study, the Data Subject’s account on the Koneksa platform is closed and any personal email or cell phone number stored by us is deleted.

## **DEVICES & DEVICE DATA**

Depending upon the Study protocol design, Koneksa may need to contract a third-party to provide Devices for use in a Study. Use of a third-party Device may require that either Koneksa or our client or their representative create an account on a vendor platform.

In the majority of cases these third-party accounts do not require information about the Data Subject to be created or operated during the Study. The Device ID assigned by the third-party vendor platform for the Device the Data Subject uses is associated with that individual’s account on our platform. Our platform is the only place in which the association between the Data Subject, the Data Subject’s account, and any Devices used by the Data Subject is maintained.

In some instances, a third-party may require an email address to create an account. In this case we will assign a Study-specific email for this account that does not identify the Data Subject.

If the Data Subject withdraws consent to participate in a Study or complete a Study, the association between the Data Subject and any Devices used as part of the Study is removed and no further data about the Data Subject is collected. Koneksa only processes data that is associated with consented Data Subjects for the period of time that consent is in effect.

If required by our contractual obligations with our clients, the ICF signed by the Data Subject will provide specific information about the Devices the Data Subject is being asked to use, the configuration of any required accounts, and how the data flows from the Device to the Koneksa platform.

## **HOW KONEKSA ENSURES DATA PRIVACY**

As the Data Processor, Koneksa does not collect any PII (except as outlined in the “Questionnaires” section). PII may be collected in accordance with Study protocol, which is defined by the Data Controller and as consented by the Data Subject by signing the ICF.

Data collected by the Data Subject (e.g., via Devices the Data Subject wears) or from the Data Subject (e.g., by completing a questionnaire) is stored de-identified in a dedicated database. De-identified means that it is not possible to identify the Data Subject as an individual. Any identifiers that are collected to support the Study protocol are stored in a separate dedicated database. Koneksa has systems, policies, and procedures in place to ensure that the overall Koneksa platform is secure and that the Data Subject’s data is kept private.

To maintain Data Subject de-identification during the data analysis and publication/presentation or results: (1) The Data Subject will be assigned a number, as names are not recorded. (2) Koneksa will save the Data Subject’s Study data by the Data Subject’s assigned number, not by name. (3) Only authorized Koneksa staff will view collected data in detail. (4) Any recordings or files will be stored in a secure location, accessed only by authorized Koneksa staff.

The Data Subject’s de-identified data may also be used/shared for the purpose of scientific and medical research separate from the purposes of the particular Study in which the Data Subject is enrolled.

## **DATA MODIFICATION**

Koneksa does not independently change data submitted by the Data Subject. We furthermore ensure that the data held within our platform is accurate and up-to-date. Koneksa will only change the Data Subject’s data, if requested by the Data Subject, upon receiving the proper authorizations from the Data Controller. All changes to data in our platform are fully tracked and recorded through a request and approval process.

## **DATA REMOVAL**

Koneksa does not delete data from our platform, unless specifically directed to do so by authorized Study sponsor personnel (acting as the Data Controller). The Data Subject may have the right to request that his/her own data be removed, based on the considerations with which the Data Subject agreed in the ICF signed by the Data Subject, which generally applies to situations where the Data Subject’s relationship with the client has ended, such as if the Data Subject withdraws consent to participate in the Study. It is important to note that this is not an absolute right, and depends on the Study retention schedule and retention requirements as set forth in applicable laws.

When the Data Subject completes participation in the Study or if the Data Subject withdraws consent, any personal identifiers we may have collected from the Data Subject as the Data Processor are removed by the Koneksa platform. The Study data the Data Subject contributed under informed consent is retained de-identified.

## **DATA ACCESS**

Data Subjects wanting to review, correct, update, delete, or otherwise limit our use of his/her personal Information that has been previously provided to us are advised to contact the Data Controller with whom the Data Subject has engaged.

## **HOW KONEKSA HANDLES PRIVACY DISPUTES**

Koneksa complies with all applicable national and international clinical and data privacy and security regulatory requirements. In particular, this includes a commitment to comply with the General Data Protection Regulation (GDPR) (beginning May 25, 2018), as well as the EU-US Data Privacy Framework, the UK Extension to the EU-US Data Privacy Framework and the Swiss-US Data Privacy Framework principles (collectively referred to as “Data Privacy Framework”).

With regard to the Data Privacy Framework in particular, Koneksa complies with the principles as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union (EU), the United Kingdom (UK), and/or Switzerland to the United States in reliance on the Data Privacy Framework Koneksa has certified to the Department of Commerce that it adheres to the Data Privacy Framework Principles with respect to such information.

For purposes of enforcing compliance with the Data Privacy Framework, Koneksa is subject to the investigatory and enforcement authority of the US Federal Trade Commission. If there is any conflict between the terms in this privacy policy and the Data Privacy Framework Principles, the Data Privacy Framework Principles shall govern. To learn more about the Data Privacy Framework program, and to view our certification, visit <https://www.dataprivacyframework.gov/>.

In compliance with the Data Privacy Framework Principles, Koneksa commits to resolve complaints about our collection or use of your personal information. EU, UK, and Swiss individuals with inquiries or complaints about our Data Privacy Framework policy should first contact Koneksa at:

Privacy Officer  
Koneksa Health, Inc.  
One World Trade  
285 Fulton Street  
Suite 77A  
New York, NY 10007  
USA

Koneksa has further committed to refer unresolved Data Privacy Framework complaints to TRUSTe, an alternative dispute resolution provider located in the United States. If a Data Subject does not receive timely acknowledgement of his/her complaint from us, or if we have not addressed the complaint to his/her satisfaction, visit <https://feedback-form.truste.com/watchdog/request> for more information or to file a complaint. The services of TRUSTe are provided at no cost to the Data Subject.

The Data Subject may have the option to select binding arbitration for the resolution of his/her complaint under certain circumstances, provided the Data Subject has taken the following steps: (1) raised his/her complaint directly with Koneksa and provided us the opportunity to resolve the issue; (2) made use of the independent dispute resolution mechanism identified above; and (3)

raised the issue through the relevant data protection authority and allowed the US Department of Commerce an opportunity to resolve the complaint at no cost to the Data Subject. For more information on binding arbitration, see US Department of Commerce's Data Privacy Framework: Annex I (Binding Arbitration).

## **HOW KONEKSA USES DATA**

Koneksa uses the data being collected on the Koneksa platform to assess the effectiveness of a Device and/or application and associated data integration into our platform; to evaluate the quality of the data; to analyze possible associations among the data aggregated from the Devices and applications; and to evaluate the effectiveness of assessments and interventions that have been offered and used with the Data Subject.

We only retain and use de-identified data for future analysis and research, to inform other study designs, for demonstration with clients or for research publication purposes.

## **HOW KONEKSA SECURES DATA**

Koneksa has implemented measures designed to secure Data Subject personal information from accidental loss and from unauthorized access, use, alteration, and disclosure.

The safety and security of Data Subject information also depends on the Data Subject personally. Where we have provided (or where the Data Subject has chosen) a password for access to the Koneksa platform, the Data Subject is responsible for keeping this password confidential. We advise the Data Subject not to share this password with anyone else.

## **HOW KONEKSA SHARES DATA**

Other third parties who support us in managing the Koneksa platform, as well as the Study of which the Data Subject is a part, may have access to the data in order to fulfill their support responsibilities. We require all third parties who have such access to the data to agree to protect it appropriately. We only share data for the purposes of the Study, as described in this privacy policy, and within the confines of our agreement with our client and the consent to which the Data Subject agreed.

We do not share data for marketing or other related purposes.

Where required, we enter into written agreements with those third-party agents and service providers requiring them to provide the same level of protection required by the Data Privacy Framework and the GDPR, and limiting their use of the data to the specified services provided on our behalf. Under certain circumstances, we may remain liable for the acts of our third-party agents or service providers who perform services on our behalf for their handling of personal data.

Koneksa does not disclose any data we may collect on a Data Subject to any other organizations, other than in fulfilling the requirement that our organization may need to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, noting that Koneksa is liable in cases of onward transfers to third parties. If this happens, we will inform the Data Controller with whom the Data Subject was engaged (for the Data Controller to contact the Data Subject), and we will comply with those requirements and will also seek to preserve Data Subject privacy as we comply.

## **HOW TO ASK A QUESTION OR RAISE A CONCERN**

As per “How Koneksa Handles Privacy Disputes” above, the Data Subject may email us at [privacy@koneksahealth.com](mailto:privacy@koneksahealth.com) or send a written letter to:

Privacy Officer  
Koneksa Health Inc.  
One World Trade  
285 Fulton Street  
Suite 77A  
New York, NY 10007  
USA

We will investigate and attempt to resolve any complaints or disputes regarding the use or disclosure of Data Subject personal data within thirty (30) calendar days of receiving a complaint. We have agreed to resolve any unresolved complaints through an independent dispute resolution process.

## **EFFECTIVE DATE**

08 April 2024