

## **PURPOSE**

This document communicates the Clinical Research Unit's ("CRU") policy regarding the European General Data Protection Regulation (GDPR) privacy law that came into effect on May 25<sup>th</sup>, 2018. The purpose of this document is to explain how the CRU meets GDPR guidelines, and how customer data is processed and protected in accordance with these guidelines. The CRU is committed to ensuring that customer data is protected and respected, by complying with GDPR requirements.

## **GDPR COMPLIANCE**

The CRU acts both as data controller and processor under GDPR guidelines but is only responsible for personal information access requests in its role as a controller. We are committed to complying with GDPR guidelines to ensure that customer privacy is protected. In addition to meeting GDPR standards, the CRU meets the legal and regulatory privacy and protection standards set out by the regions in which the CRU operates.

## **PRIVACY AND SECURITY MEASURES**

The CRU employs a variety of privacy and security procedures to safeguard and secure the personal information we collect. These security measures ensure that the existing privacy laws and regulatory standards are met. Security measures include, but are not limited to:

- Data Security: end-to-end encryption using SSL technology with high-grade 256-bit encryption protects data "in transit" for privacy, integrity and authentication. Access control is achieved by the means of authentication and authorization. Data at rest is stored in encrypted format using the industry-standard AES-256 algorithm. Data is logically segregated from application access
- Security: In-depth security including firewalls and access control lists (ACLs); network and host-based intrusion detection; scanners; authentication, authorization, and accounting (AAA), and encryption are used as appropriate.
- Applications Security: Role-based user privileges ensure user only access to the appropriate application functionality. Multi-Factor Authentication (MFA)/ Two-Factor Authentication (2FA). Inactivity automatic access suspension.

## **DATA WE COLLECT**

The CRU collects and processes the data provided by the study team as part of a research study, which may include your personal data and data concerning health.

This data is being collected and processed with your consent.

### WHY WE COLLECT THIS DATA

The CRU collects and processes this data for the purposes of delivering services in support of clinical research. We will only collect and process the data you provide for the purposes discussed by the study team and to ensure compliance with regulatory requirements.

The CRU will not sell, transfer, or disclose your data to a third party, except to contractors performing activities directly related to the purpose for which the data was collected, and to comply with regulatory auditing or monitoring requirements or as required by law.

### HOW LONG WE KEEP THIS DATA

The CRU only saves data for as long as it is needed, and as required by regulation. When a study team informs us that the study is complete, we will store a backup of the collected and processed data. We will delete the backup after one year, unless we are required by regulation or law to retain the data longer.

### ACCESS, CORRECTIONS, OBJECTIONS AND DELETIONS TO PERSONAL DATA

You still have rights over what happens with your data being held by the CRU.

Every user has the right to the following:

- Access: You have the right to request that the CRU provide copies of your data in our possession.
- Rectification: You have the right to request that the CRU correct any data you believe to be inaccurate and complete any data you believe to be incomplete.
- Erasure: You have the right to request that the CRU erase your data in our possession, under certain conditions.
- Restrict processing: You have the right to request that the CRU restrict the processing of your data in our possession, under certain conditions.
- Object to processing: You have the right to object to the CRU processing your data, under certain conditions.
- Data portability: You have the right to request that the CRU transfer the data we have collected to another organization or directly to you, under certain conditions.
- Withdraw consent: You have the right to withdraw your consent for the CRU to continue collecting and processing your data. Withdrawing your consent will not affect the collecting and processing of your data prior to withdrawal.

If you would like to exercise any of these rights, please contact us at our email: [cru@ucalgary.ca](mailto:cru@ucalgary.ca).


### ***Restrictions to the Right to be Forgotten***

The CRU follows the Good Clinical Practice for clinical research. The guidelines on data and record management prohibit the deletion of clinical research data. The CRU reserves the right to retain and disclose your data, which may include your personal data, as permitted or required by law or regulation, and in accordance with these guidelines.

### **HOW TO CONTACT US**

If you would like to speak to us about how GDPR law impacts your personal data at the CRU, or have any requests for information about, corrections to, or deletion of your data, please send requests to: [cru@ucalgary.ca](mailto:cru@ucalgary.ca)

Any updates to this GDPR statement will be posted to our website [www.cru.ucalgary.ca](http://www.cru.ucalgary.ca)

Approvals			
Approved By:	 Tracy Wang, Director of Strategy and Operations	Date:	June 29, 2022

Document version	2.1
Date	June 29, 2022
Prepared by	Matt Szostakiwskyj, Regulatory and Compliance Analyst
Approved by	Tracy Wang, Director of Strategy and Operations