Data Privacy & Security for Emulate Software Applications

Overview

At Emulate, data privacy and security are among our highest priorities, which is why we work to ensure that user data generated when working with any Emulate software is as protected as possible. Using Emulate's suite of software to remotely control experiments, plan studies, or analyze results involves creating and interacting with numerous types of data. This document provides a brief overview of these data types as well as encryption, storage, access, and privacy policies. Our data policies are designed with privacy in mind at every step, ensuring your sensitive data is secure when using Emulate's software and technology.

Emulate Software Applications

Software Applications

Emulate's suite of software applications allows users to remotely control Zoë-CM2, precisely plan out and execute experiments, and conveniently analyze data. These web applications include:

Type	Description
Zoë Manager	Remotely monitor and control the experimental parameters of Zoë-CM2.
Study Manager	Manage the execution of Emulate cell culture protocols and track results.
Data Analysis	Analyze results with calculators based on continuous flow. Score and grade images.

emulate

Data Types

Description	Below are the different types of data involved in user interactions with Emulate's suite of software.
Account Data	Account Data, which includes a user's name, email, password, and company name, is required to create a user account. This information is linked to a cohort, or a group of at least one user and a Zoë. Account Data is required to authenticate the user to Zoë Manager, Study Manager, and Data Analysis.
Instrument Data	Instrument Data is information about the operations of, and user interactions with, the combination of a Zoë-CM2, an Orb, and a set of Organ-Chips. This includes network information, the unique instrument ID, the corresponding cohort, a timestamp of operations, as well as settings and parameters used. Actual recorded Start/Stop Events (as opposed to those planned and set by the user before the experiment) are a type of Instrument Data captured with the associated settings and parameters. For example, starting flow records the time, flow rate, and planned duration. During Zoë operation, pressure, temperature, and other sensor and system data are captured and stored on the instrument and—if it is connected to the internet—in the cloud application.
Telemetry Data	Telemetry Data is anonymized metadata about the operations of a Zoë and its interactions with the Emulate software. This data is recorded through our suite of applications and includes timestamps of interactions with Zoë, frequency of messages sent, online status, user interactions with Zoë Manager, and the interactions with on-screen display and web UI.
Study Data	Study Data is information about the experiments created in Study Manager and run on a Zoë. This includes the experimental design, allocation of chips, timeline of events, organ model selections, and any plans for the combinations of flow rate and stretch parameters that are set by the user on Study Manager before running them on Zoë. This information is captured by the suite of applications and linked to the study.

emulate

Data Storage

Cloud Storage

Emulate software applications utilize Amazon Web Services (AWS) to house databases, store files, enable instrument messaging, and control notifications. For Emulate and Emulate customers, AWS provides the following benefits: highly secured data centers with SOC2 AND ISO27001 compliance; geographically spread infrastructure to store data close to the customer to improve performance and user experience; redundancy of all hardware components; and a commitment to security standards and regulations. A user's email, name, company, and login history are managed with OneLogin.

Encryption

Data in transit from the user to Emulate's suite of applications is encrypted using Transport Layer Security (TLS) encryption. Additionally, all data transferred between a Zoë-CM2 and online services are authenticated and encrypted using TLS. Files in AWS are stored in an encrypted AWS Simple Storage Service (S3) using AES 256-bit encryption.

Account Data Storage

Account Data is stored in US databases. Sensitive information, such as a user's password, is sent from the user's computer when they enter their username and password into the Zoë-CM2 login form for authentication purposes. Account Data is exchanged with the web browser during user interactions. No user's Account Data is transferred to or from the instrument.

Instrument Data Storage

Instrument Data is stored in US databases. It is transferred from the instrument during operation and to the user during their interaction with Zoë Manager, Study Manager, or Data Analysis web applications.

Telemetry Data Storage

Telemetry Data is stored in US databases. It is captured from the interactions between the user, the instrument, and the suite of applications. Emulate only actively stores data necessary to track instrument operation and performance.

Study Data Storage

Study Data is stored in US databases. It is transferred to the instrument after a user has associated the instrument with a study in Study Manager, and it is sent between the user and the database during the user's interaction with Study Manager, Data Analysis, or Zoë Manager.

Backup

Backup copies are taken of all Account Data and Study Data in the database. These snapshots are encrypted and stored securely and separately from the database housing the data. Backup copies are also taken of all the user-submitted files.

Limitations

While cloud storage provides an extremely secure method of storing data, there are a few infrequent and minor accessibility limitations. For instance, there may be downtime when Emulate updates any of the applications. Downtime may also occur for AWS itself which, although extremely rare, affects essential systems; however, Zoë operations will remain unaffected.

Data Access

Privacy by Design

Emulate recognizes that the software applications and Zoë-CM2 are used in sensitive experiments that involve confidential data. As such, all Study Data, Instrument Data, and Account Data are private to the associated cohort by default. In some cases, Emulate's cloud administrators do collect metadata—including data about user logins, instrument activity, and start-and-stop events—in an aggregate "Users per Day" report to monitor system performance and note any potential improvements to the user experience. However, those outside of a cohort cannot view individually identifying data. In the aggregation process, Emulate does not look at the specific content of data associated with experiments, including images, experiment names, compounds, etc.

Account Data Access

A cohort's administrator, called an "Org admin," can view all Account Data of the users in their cohort (other than passwords); however, other users in the cohort cannot view other members' Account Data, aside from that which is shared on studies. The Org admin can disable or delete individual accounts from a cohort, though usernames will be retained in the audit log. Emulate can view the company name in the cohort list and see the username and email when creating new accounts; otherwise, Emulate cannot view Account Data unless given direct permission by the account owner for maintenance. Emulate may gather Account Data in an anonymized aggregate for quality assurance purposes, in which case only anonymous identifiers are visible.

Instrument Data Access

Users can view their instrument's available data through Zoë Manager. The Emulate Field Engineering team may access additional Instrument Data for a support request if granted access by the Org admin. Emulate's policy is to only view individual Instrument Data when providing customer support; however, Emulate may gather Instrument Data in an anonymized aggregate for quality assurance purposes.

Telemetry Data Access	Telemetry Data cannot be viewed by the user, as it is only available to Emulate for quality assurance reasons.
Study Data Access	Individual Study Data may only be viewed by members of the cohort. Emulate cannot view individual Study Data unless granted access by a user within that cohort (to assist with Zoë or experiment troubleshooting, for example). For any study, a limited amount of information about the organ protocol selected, the flow rate chosen, and the types of chips used is accessible by Emulate for quality assurance purposes; however, all other information about the specifics of the study is invisible to Emulate unless cohort members grant permission.

Regulations & Compliance

Disclaimer	Zoë Manager, Study Manager, and Data Analysis web applications are intended for research use only. The platform is not governed under HIPAA regulations and is not validated for use in diagnostic procedures.
Removing User Data	Account Data will be removed if a user closes their account, and all associated data will be deleted (other than the user's first and last name, which are retained in the audit log). User-submitted information—such as images, comments, and changes—belongs to the cohort and will not be removed if a user deletes their account. If a company requests that a cohort be removed, Emulate can remove all Study Data, as it belongs to the cohort. Instrument Data cannot be deleted, but it can be anonymized by disassociating Zoë from the cohort.
External Resources	**OneLogin:** onelogin.com/compliance **Amazon Web Services:** aws.amazon.com/products/storage/