OpenCap Data and Privacy

This privacy statement explains how OpenCap collects, uses, disclose, and otherwise processes personal information in connection with our OpenCap platform. This document also provides information to aid in incorporating OpenCap into IRB-approved research studies. Our platform includes:

1. The OpenCap website
2. The OpenCap web application
3. The OpenCap smartphone application
4. Application program interfaces

Please contact us at info@opencap.ai if you have any questions after reading this document and viewing the corresponding links.

Data Security and Data Flow

The security, integrity, and confidentiality of your information are extremely important to us.

The Stanford University Privacy and Security Offices reviews research projects conducted at Stanford that handle High Risk Data (e.g., video data that is considered protected health information [PHI] in some instances). The office has certified OpenCap to be compliant with the Stanford University Minimum Security Standards for Infrastructure-as-a-Service Solutions. The details of these requirements can be found here. Part of these standards ensures that OpenCap is HIPAA compliant. OpenCap can be used in the US, European Economic Area, the United Kingdom and Switzerland when a relevant agreement is in place with Stanford University.

The most up to date privacy and security terms for OpenCap can also be found on our website's terms and conditions.

All video and processed data are encrypted in transit and at rest (i.e., while stored). The flow of data can be seen in Figure 1. More details on data and data flow are below:

- All videos have humans in them, so they are assumed to contain Protected Health Information (PHI) under US HIPAA Privacy Rule if it is created, received, maintained or transmitted on behalf of a HIPAA covered entity. The processed movement data is de-identified (pseudonymized).
- All data transfers, denoted by arrows, use an https protocol and thus have TLS 1.2 encryption.
- All Amazon Web Services (AWS) services (EC2 instances, S3) are through a Stanford AWS account, covered by an AWS Business Associate Agreement (BAA) and GDPR Standard Contractual Clause ensuring HIPAA and GDPR compliance for handling such data.
- Any request to upload or download data from S3 requires authentication through the API, using a 20+ character password and 2-step authentication.

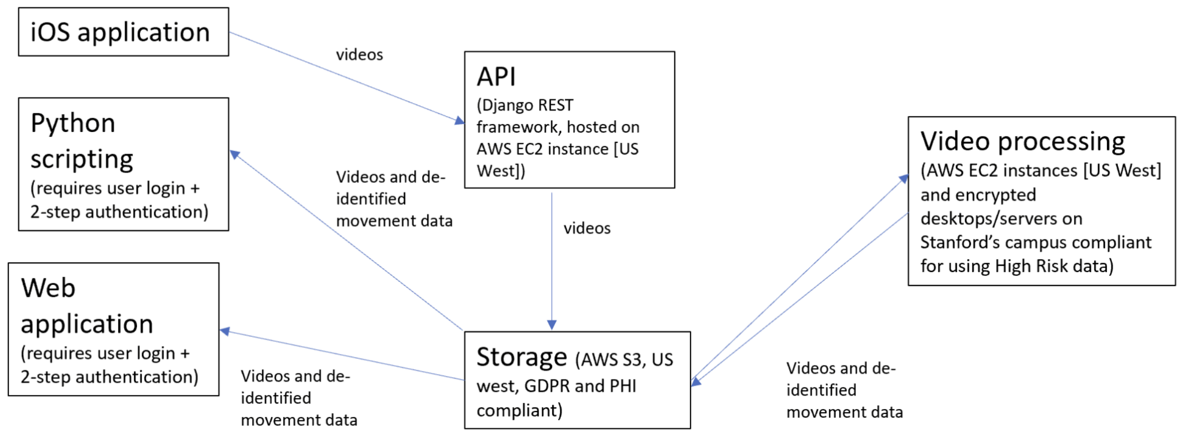
iOS application
videos
API
(Django REST framework, hosted on AWS EC2 instance [US West])
Python scripting
(requires user login + 2-step authentication)
Videos and de-identified movement data
videos
Video processing
(AWS EC2 instances [US West] and encrypted desktops/servers on Stanford's campus compliant for using High Risk data)
Web application
(requires user login + 2-step authentication)
Videos and de-identified movement data
Storage (AWS S3, US west, GDPR and PHI compliant)
Videos and de-identified movement data

Figure 1: Data flow for videos and processed movement data in OpenCap.

What personal information do we collect?

When you use our software to conduct your research study, OpenCap collects and processes the following information:

Information about you (the investigator):

- Information you provide when creating an account (i.e., name, email, etc.)
- Device information, including IP address
- Site and app usage data

Information related to the participants of your study:

- Participant demographic information (height, weight, sex, gender, month and year of birth)
- Videos of motion of interest
- Processed movement data (i.e., the time-history of how body segments are moving during the motion of interest)
- Additional characteristics that you may provide about the participant and trial, including the presence of movement conditions (e.g., osteoarthritis) or the type of movement being performed (e.g., climbing stairs)

In addition, where participants are minors, personal information includes data about minors.

How will we use this information?

Data protection legislation requires that we meet certain conditions before we are allowed to use your data in the manner described in this statement, including having a "lawful basis" for the processing. The basis for processing could be one or more of the following:

- **Consent** - Your participants have provided explicit consent for the processing of their data, including parental / guardian's explicit consent for minors;

- **Contract** - The processing is necessary for the performance of a contract with you or in order to take steps prior to entering into a contract with you;
- **Legal obligation** - The processing is necessary for us to comply with legal and jurisdictional obligations to which we are subject such as keeping accounting records;
- **Legitimate interests** - The processing is in our legitimate interests or the legitimate interests of a third party, which are not overridden by the data subject's interests and fundamental rights and freedoms.

We may use this information to:

1. deliver our services to you in support of your study and to provide you with information about study participants;
2. detect, investigate, and prevent activities that may violate our policies, pose safety issues, or be fraudulent or illegal;
3. improve algorithms; and
4. compile and share aggregated movement characteristics.

Data storage, retention, and destruction

Videos are collected by the smartphone application, then are uploaded to S3 through the API, where they are encrypted in storage. Backend servers/desktops download these videos from S3 and process them into de-identified movement data, which is uploaded to S3. These backend machines are encrypted and approved at Stanford for high-risk data. Users, who have logged into the web application can view and download their videos and processed de-identified movement data. Python scripting also enables data download, after users log in for authentication. Data is stored in S3 and potentially on encrypted computers at Stanford for development purposes. Data is also backed up in S3 in a different region.

If a participant requests to have their data removed, you (the investigator) can delete their data from the OpenCap dashboard. Otherwise, data will be retained for a period of 50 years, to allow investigators to reanalyze and verify the results of published investigations. Data that participants consent to share publicly will not be deleted, unless a participant requests their data be removed.

Who has access to the data?

In summary, the OpenCap development team and the Stanford Neuromuscular Biomechanics Lab will have access to the data. Prior to each data collection, the investigator (i.e., the OpenCap account holder) will ask the participant to what degree they would like to share their data via an informed consent process. The options available in OpenCap range from sharing only with Stanford to public sharing of all data. Investigators must include these data access and sharing options on their consent forms, and enter the appropriate sharing selection when processing each participant.

Items required when incorporating OpenCap into an IRB-approved study

As investigator, you are required to complete the following steps when using OpenCap:

1) Inform participants that their data will be shared with researchers at Stanford to improve algorithm research and development. For example:
    a) I understand that my videos and movement data (i.e., the time-history of how my body segments are moving when I walk or perform other movements) will be shared with the OpenCap research and development team. Sharing my data will help improve the algorithms used in OpenCap, and enable future progress in human motion science. The videos and motion data will be stored on a secure server and will not be linked with any other identifiable information about me.
    b) I understand that I can request my data be removed by contacting the study investigator.
2) Include a data sharing opt-in option on the consent form. E.g.,

    How would you like to share your video and biomechanics data?
    a) share no data publicly
    b) share processed motion data
    c) share de-identified data (videos with face blurring and motion data) publicly
    d) share videos (without face blurring) and de-identified motion data publicly
3) For studies that are subject to HIPAA, in the HIPAA release, write that “the development team for the OpenCap biomechanics tool has access to videos and de-identified demographic and movement data. This team will make your data publicly available in accordance with your data sharing preferences.”
4) Include in the risks section of the IRB application and consent form:

    “The investigators do not have control over the secondary use of data that the participant agrees to share publicly.”
5) Data storage section of application:

    “Video and biomechanics data are collected using the OpenCap web application. This tool is hosted by Stanford University, is HIPAA and GDPR compliant, and complies with Stanford University requirements for Infrastructure-as-a-Service Solutions that involve high risk data, like videos. All data are encrypted in transit and at rest and can only be accessed by the OpenCap development team and the investigator. Authentication with a 20-character password and two-factor authentication is required to access data.”

The use of AI in data processing

AI is not used for automated decision making. We use AI to compute the location of key locations on the body (e.g., the center of the ankle, the foot) from the recorded smartphone videos. We have tested the accuracy of using this AI approach to gold-standard techniques conducted in a “traditional” laboratory. We continuously benchmark our AI system to gold-standard, non-AI processed data.

What are my rights?

Under certain circumstances, you have rights under the data protection laws that apply to you in relation to your Personal Information. Please refer to Stanford University Online Privacy Policy. To exercise, please contact your study investigator.

Changes to our privacy statement

We may modify this statement from time to time. When we make substantive changes to this statement, the latest update will be included on our website. Your further use of our Services after a change to our statement will be subject to the updated statement. If you don't agree to the changes, then you can always stop using our services, delete your account and stop giving us any more personal information.

This Privacy Statement is effective as of the date it is provided to you or October 12, 2023, whichever is earlier.

For additional information regarding our privacy policy, please refer to Stanford University Online Privacy Policy.