Physitrack Limited

6th Floor, 125 Wood Street
London EC2V 7AN

UK Company House registration 8106661
UK ICO registration ZA396165
VAT GB183639673

CEO: Henrik Molin
CTO: Nathan Skwortsow

support@physitrack.com

Datenschutz und Sicherheit

Physitrack Telehealth ist darauf ausgerichtet, die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Kundendaten zu schützen.

Verschlüsselung von Anrufen

Video- und Audioströme zwischen den Gesprächsteilnehmern werden mit AES 256-Bit-Verschlüsselung verschlüsselt. Dies schließt die gemeinsame Bildschirmnutzung ein.

Speicherung der Daten

- Physitrack nimmt weder Audio noch Video auf.
- Die einzigen Daten, die wir speichern, sind Daten über Ihren Anruf (so genannte Metadaten), wie z.B. die Startzeit, die Endzeit, die Dauer, den Namen des Kunden, mit dem Sie gesprochen haben, usw.
  Dies soll Ihnen helfen, Einblicke zu erhalten und Ihren Kunden Rechnungen stellen zu können. Außerdem können wir die Funktion unserer Plattform so technisch überwachen und Probleme lösen.
- Ihre Daten werden sicher in unserem ISO 27001 und SOC2 zertifizierten Rechenzentrum gespeichert.

DSGVO:

Welche Arten von Daten werden von Physitrack erfasst?
Physitrack ist eine Plattform, die von Grund auf auf Datenschutz und Sicherheit Ihrer eigenen Daten und der Ihrer Kunden ausgerichtet ist. Alle Richtlinien und technischen Standards folgen diesem Prinzip. Darüber hinaus ist Physitrack nicht in der Lage, Daten an Dritte weiterzugeben. Unsere Einnahmen stammen schlicht und einfach aus Abonnements und Unternehmensfunktionen.

• Physitrack führt seine Anwendungen und Datenbanken auf Amazon Web Services (AWS) aus. AWS betreibt die vielleicht sichersten Rechenzentren der Welt.
• Daten werden in einer Datenbank gespeichert, die im selben Rechenzentrum ("Verfügbarkeitszone") wie der Server gehostet wird, auf dem Sie Physitrack verwenden. Wenn Sie beispielsweise us.physitrack.com verwenden, befinden sich sowohl die Anwendung als auch die Datenbank in den USA. Wenn Sie uk.physitrack.com verwenden, befinden sich sowohl die Anwendung als auch die Datenbank in der EU.
• Sensible Felder werden "in Ruhe" (wenn sie "dauerhaft" gespeichert sind) in der Datenbank sowie "im Flug" (wenn sie zwischen Ihrem Browser / Gerät und unserer Anwendung übertragen werden) verschlüsselt.
• Physitrack erstellt zwei Arten von Datenbanksicherungen: eine Echtzeitsicherung und eine Sicherung, die alle 24 Stunden durchgeführt wird. Diese Sicherungen werden in einem anderen Rechenzentrum als die Online-Datenbank gespeichert, um Datenverlust im Katastrophenfall zu vermeiden.
• Backups werden verschlüsselt.

In der folgenden Liste ist aufgeführt, welche Art von Daten wir speichern.
Beachten Sie, dass Physitrack keine Kreditkarteninformationen auf unseren Systemen speichert.

GDPR: What types of data are collected by Physitrack?

Physitrack is a platform designed from the ground up around privacy and security of both your own and your clients' data. All policies and engineering standards follow this principle. Further, Physitrack is not in the business of sharing data with third parties. Our revenue comes from subscriptions and enterprise features, plain and simple.

- Physitrack runs its applications and databases on Amazon Web Services (AWS). AWS operates perhaps the most secure data centers in the world.
    - Amazon Web Services, Inc.
      410 Terry Avenue North
      Seattle WA 98109
      United States

- Data is stored in a database that is hosted in the same data center ("availability zone") as the server on which you use Physitrack. For example, if you use us.physitrack.com, both the application and the database are in the US, and if you use uk.physitrack.com, both the application and the database are in the EU.
- Sensitive fields are encrypted "at rest" (when stored "persisted") in the database as well as "in flight" (when being transferred between your browser/device and our application).
- Physitrack makes two types of database backups: a real-time backup and a backup that is made every 24 hours. These backups are stored in a different data center from the online database to avoid data loss in case of a catastrophe.
- Backups are encrypted.

The list below enumerates what type of data we store.

> Note that **Physitrack does not store any credit card information on our systems**.
> Payments are processed by Adyen, our payment processor.

Practitioner data

Field name	**Description**	**3rd party processors** *Note that all data is also processed by AWS*
First & last name		Adyen, Chargebee, Customer.io, Helpscout, Twilio
Email address		Adyen, Chargebee, Customer.io, Mailchimp
Owner	Which PT Direct account owns this practitioner?	Adyen, Chargebee, Customer.io
Practice name		Adyen, Chargebee, Customer.io

Field name	**Description**	**3rd party processors** *Note that all data is also processed by AWS*
Address		Adyen, Chargebee,
Country		Adyen, Chargebee, Customer.io
State		Customer.io, Chargebee
Skype ID		
Mobile phone		Twilio
Timezone		Customer.io
VAT ID		Chargebee
Agreed to terms of service?		
Subscription status		Customer.io
App preferences	E.g. weight units, notification preferences	
Password	*Encrypted*	

Field name	**Description**	**3rd party processors** ***Note that all data is also processed by AWS***
Affiliation	Practice management system or organization	Customer.io
API integration	Patient management system (PMS) and api key for the Physitrack-connection to the PMS	Customer.io (only the name of the PMS, not the key)
Attempted logins	Timestamp and IP address of unsuccessful login attempts	
Custom templates	Custom templates created by this practitioner	
Messages	*Encrypted.* Messages sent to and received from clients.	
Video call log	Logs (timestamp and duration, not contents) of video calls	
Sign in count		Customer.io
Last sign in date & IP		Customer.io (only timestamp)
Current sign in & IP		

Field name	Description	3rd party processors *Note that all data is also processed by AWS*
Creation date		Customer.io
Date record was last updated		
Search settings	Recent search settings	
Custom exercise videos and images		Coconut, Algolia, Customer.io (only count)

Client data

Field name	Description	3rd party processors
First & last name		-
Gender		-
Year of birth		-
Mobile phone		Twilio
Email		Mailchimp

Field name	Description	3rd party processors
Access code & exercise program	Access code and exercise program with its content (exercises and/or educational content and/or outcome measures).	Google Firebase, Fabric.io, Twilio
Outcome measures	*Encrypted*. Answers to outcome measures.	-
Messages	*Encrypted*. Messages sent by and to the client, exercise feedback.	-
Video call log	Timestamp and duration of made video calls.	Voxeet
Video call audio	*Encrypted.* If enabled by the practitioner, an mp3 audio recording of made video calls.	Amazon Web Services
Adherence details	*Encrypted*. Details of the completion of sets, reps, hold, pain level, etc.	-
Diagnosis code	*Encrypted*. Optionally, a practitioner may choose to store diagnosis codes on Physitrack.	-
Custom exercise videos and images	*The practitioner is prevented from entering the client's first and last name in the exercise title or description.*	Coconut, Algolia

> **Access code & client-identifiable information**
>
> As soon as an access code contains patient-specific information (e.g. messages, outcome measures or exercises featuring this patient), the client must enter their year of birth to access the exercise program.
>
> Only a certain amount of incorrect attempts can be made every hour before PhysiApp is locked.

Third party vendors that process data on behalf of Physitrack

- **Adyen** (GDPR-compliant, data processing agreement in place)
  We use Adyen to process our payments.
  No client data is processed by Adyen.
- **Algolia** (GDPR-compliant, data processing agreement in place)
  We use Algolia to power our free-text search of exercises.
  No practitioner or client data is processed by Algolia that could let Algolia identify practitioners or clients.
- **Amazon Web Services** (GDPR-compliant, data processing agreement in place)
  Physitrack owns and controls logical access to the infrastructure maintained by AWS, while AWS maintain the physical security of the servers, network and the data center.
- **Coconut** (GDPR-compliant)
  We use Coconut to transcode all videos into web/mobile viewable formats. No patient information is sent to Coconut, but the videos sent to Coconut for encoding may contain videos that feature a client. Coconut automatically *deletes all uploaded content* after 24 hours.
- **Cloudflare** (GDPR-compliant, data processing agreement in place)
  We use Cloudflare for DNS and content distribution. Cloudflare uses enhanced privacy protocols for DNS over TLS and DNS over HTTPS which prevents data tracking by not linking DNS queries to your personal IP address (personal data) and limits record any retention to 24 hours
- **Chargebee** (GDPR-compliant, data processing agreement in place)
  We use Chargebee to help manage our subscription process and invoicing. Information sent to Chargebee includes the practitioner's billing information such as name, email and payment method. No patient information is sent to Chargebee.
- **HelpHero** (GDPR-compliant)
  We use HelpHero to show onboarding tours to practitioners in the demo version of Physitrack, and to practitioners who have not yet added any clients.
  No practitioner or client data is processed by HelpHero.
- **Helpscout** (GDPR-compliant, data processing agreement in place)
  We use Helpscout to process customer support emails and display our online knowledge base (such as the one you are looking at).
  On the web version of Physitrack, when a practitioner sends a message to Helpscout,

Helpscout processes the IP address, name and email of the practitioner.
Both practitioners and clients have the possibility to send a support email to support@physitrack.com or support@physiapp.com which will be displayed to a qualified Physitrack staff member.
We tightly control who has access to Helpscout, and require 2-factor authentication.

- **Mailchimp** (GDPR-compliant, data processing agreement in place)
  We use Mailchimp's "Mandrill App" service to send transactional emails such as passwords and access codes. The recipient email and subject line are stored by Mailchimp, but message body is not.

- **Google Analytics** (GDPR-compliant, data processing agreement in place)
  We use Google Analytics on our marketing site and on our app, but only for practitioners who are not logged in.
  No practitioner data is processed by Google Analytics other than the customary tracking information, such as screen resolution, ip address, browser, etc.
  No client data is processed by Google Analytics other than the customary tracking information, such as screen resolution, ip address, browser, etc.

- **Google Firebase** (GDPR-compliant, data processing agreement in place)
  We use Google Firebase to detect whether a client or a practitioner is online.
  No data is processed by Google Firebase which would allow a third party to identify who the parties are.

- **Google G Suite** (GDPR-compliant, data processing agreement in place)
  We use Google G Suite to host our email. All @physitrack.com emails are processed by Google G-Suite on behalf of Physitrack.

- **Customer.io** (GDPR-compliant, data processing agreement in place)
  We use Customer.io to send onboarding emails to practitioners.
  The information that is sent to Customer.io is limited to the information that is required to properly identify the correct recipients of our various onboarding emails, and includes activity information such as name, email, the number of patients, number of assigned exercise programs, subscription information.
  No client data is processed by Customer.io.

- **Data Dog** (GDPR-compliant, data processing agreement in place)
  We use Data Dog to monitor and improve performance of our application and infrastructure.

- **Sentry** (GDPR-compliant, data processing agreement in place)
  We use Sentry to track errors in our source code.

No practitioner or client identifiable data is processed by Sentry, as this data is scrubbed before it gets sent.

- **Fabric.io** (GDPR-compliant, Data Processing Terms)
  We use Crashlytics, a product by Fabric.io (which in turn is owned by Google) to track crashes and bugs inside our iOS and Android apps.
  For clients, the access code is processed by Fabric.io to let us more quickly find bugs.
  For practitioners no personally identifiable information is processed by Fabric.io.

- **Transifex** (GDPR-compliant)
  We use Transifex to dynamically translate our marketing site. Transifex places cookies to remember which language you are viewing the Physitrack marketing site in.
  No practitioner or patient data is sent to Transifex.

- **Twilio** (GDPR-compliant, data processing agreement in place)
  We use Twilio to send access codes via SMS to clients and send various notifications via SMS to practitioners.

- **Typeform** (GDPR-compliant)
  We use Typeform to collect troubleshooting information from practitioners and their clients.

- **Voxeet** (Dolby) (data processing agreement in place)
  We use Voxeet to help power our video calling functionality. Video streams are encrypted using AES-128 bit encryption or stronger.
  Only the practitioner and patient names and IP addresses are processed by Vxoeet. Any text chat messages during a video session are ephemeral, and destroyed after the session closes.

> **Note:** healthcare practitioners may choose to automatically share adherence details and exercise program information from Physitrack to their patient management system.
> This is done at the discretion and under the control of the clinic or healthcare practitioner.