MONSENSO

Product sheet

## DATA MANAGEMENT & DATA SECURITY

**Monsenso Data Management overview:**

- European General Data Protection Regulation (GDPR)
- Local country law, hereunder Danish Act on Processing of Personal Data & Guidance to Executive Order on Security
- ISO 27001 & 13485 certified
- CE Class I Medical Device & TGA
- HIPAA compliant & FDA excempt

**Our hosting partner Data Management overview:**

- ISO 27001, SOC 1 Type II & SOC 2 Type II certified
- PCI DSS Level 1 certified & Cloud Security Alliance compliant

### OVERVIEW

The Monsenso mHealth solution for mental illnesses is a CE, class I, medical device, elevating itself from other mental health applications available.

The system collects and maintains a range of data from and regarding the users, which are securely stored in the system.

The Smartphone application used by the individual can collect 'objective' and 'subjective' data; the 'objective' data is collected through the Smartphone's built-in sensors and linked wearables, whilst the subjective data can be gathered through daily self-assessments, questionnaires, as well as rating performed by the professional.

Furthermore, data on medication intake, plans, clinician's notes and other information can be entered into the system, if modules are enabled.

The sensor data collected from Smartphones and wearables may vary depending on configuration as well as make and model, but it will typically include data related to:

- Social activity, which is a combination of telephone activity (number of calls, duration, type) and text messaging activity (length, timestamp, protocol)
- Physical activity, collected from eg. the accelerometer and/or step counter
- Sleep, such as length, light or deep sleep, and the number of wake-ups during the night
- Phone activity, in terms of eg. general usage, power level, ambient light, proximity, screen activity, and app use
- Mobility, such as GPS, Cellular network, Bluetooth and Wi-Fi
- Speech patterns, such as pitch, tone, and entropy

All the information collected through the system can be accessed by both individuals and professionals, depending on permission level, which is configurable throughout the solution.

All data collection follows user licence agreements for customers and users, and varies depending on configuration. Consent from users is obtained through the signup process, accepting both the Data Privacy Policy, as well as the End User Terms & Conditions, before gaining access to the solution.

## DATA SECURITY

Transmission of information from the Smartphone to our data centre is performed via the internet, and apply strong encryption using 'Perfect Forward Secrecy' TLS 1.2 protocol, and data stored on our servers is encrypted using RSA 4096 bit keys.

A user can request to have all his data deleted at any point in time through a written request to Monsenso, or through the 'delete' feature in the account management section in the web portal.

## ACCESS MANAGEMENT

Access management conforms to the Danish Guidance to Executive Order on Security, including support for:

- Access control – The users are reviewed every six months, where inactive users are disabled
- Denial of access – A user will be denied access after five unsuccessful consecutive login attempts and an client / IP will be denied access after 20 consecutive failed login attempts
- Logging – Monsenso logs all transactions in the system, including information on data operation, data items, IP number, user id, and timestamps

## HOSTING PROVIDER

Monsenso's hosting provider is OVH, a French certified hosting company. It is a technical service provider, which supplies the infrastructure to host our customer's data. Data is stored in OVH's French data centres where all data is encrypted, hence OVH have no access to data.

All physical access to the OVH premises is strictly monitored, and employee access rights are re-assessed regularly, according to their remit. To prevent any intrusions or hazards, every boundary is secured using barbed-wire fencing, and video surveillance and movement detection systems are in continuous operation. Activity within the data centres and outside the buildings is monitored and recorded on secure servers, while surveillance teams are on site 24/7.

In the event of a technical incident, they will react immediately to ensure that the server is repaired as quickly as possible. The OVH data centres are powered by two separate electrical power supplies and are also equipped with UPS devices. Power generators have an initial autonomy of 48hrs to counteract any failure of the electricity supply network. Every data centre room is fitted with a fire detection and extinction system, as well as fire doors.

OVH is is ISO 27001 certified, and relies on the ISO 27002 standards to implement good practices in terms of information security management, and ISO 27005 to perform its risk assessment and associated processing. Further, SOC 1 Type II attests that OVH has well defined and implemented controls for the protection of its customers' data, while SOC 2 Type II evaluates its controls against the international standard established by the American Institute of Technology (AICPA) Certified Public Accountants, in its principles on Trust Services Principles.