MONSENSO

Fact sheet

DATA MANAGEMENT

DATA PROTECTION AND SECURITY

Monsenso is an innovation leader in digital health for mental illnesses. Our mission is to empower and inspire individuals, caregivers and care providers, to improve mental health and help society overcome the burden of mental illnesses.

www.monsenso.com

Fact sheet

DATA MANAGEMENT

DATA PROTECTION AND 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
- Cyber Essentials certified
- CE Class 1 Medical Device & TGA
- FDA exempted

Hosting partner Data Management

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

OVERVIEW

The Monsenso digital health solution for mental illnesses is a Class 1 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 is 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 ratings performed by professionals.

Furthermore, data on medication intake, plans, clinicians' 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 the configuration, but will typically include data related to:

- Physical activity, collected from the accelerometer and/or step counter
- Sleep, such as length, light or deep sleep and the number of wakeups during the night
- Phone activity, in terms of e.g., power level, ambient light (Android only), screen activity (Android only)
- Mobility (GPS-location)

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

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

WEARABLES DATA COLLECTION

When a user connects their Withings' account to Monsenso, some of their historical and future data will be collected. The system collects the following endpoints:

- Activity - Provides daily aggregated activity data of a user. Example of persisted data: Step count, elevation, distance, etc.
- Measurements - Provides measures stored on a specific date, such as weight, height, fat-free mass, temperature
- Sleep - Provides the user's night sleep measures with details of each phase of their sleep cycle.

DATA MANAGEMENT
DATA PROTECTION AND SECURITY

- Sleep summary, such as the total time slept, wake up count, REM sleep, light sleep, deep sleep, etc.

DATA SECURITY

The transmission of information from the smartphone to our data centre is performed via the internet. Strong encryption is applied using 'Perfect Forward Secrecy' TLS 1.2 protocol and all data stored on our servers is encrypted using RSA 4096-bit keys.

HOSTING PROVIDER

Monsenso's hosting provider is OVH, a French certified hosting company. OVH is a technical service provider, supplying the infrastructure to host our customers' data. The data stored in OVH's French data centers is encrypted, leaving OVH without access to our data.

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

In the event of a technical incident, OVH 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 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 fire detection and extinction system, as well as fire doors.

OVH 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. SOC 2 Type II evaluates its controls against the international standard established by the American Institute of Technology Certified Public Accountants (AICPA) applying its principles on Trust Services Principles.

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 a 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.