MedsOnTrack
Data Policy

Data Service

The data service is hosted in Microsoft Azure, all security and compliance certification apply to service and the data contained in it. They currently are:

1. ISO/IEC 27018
2. ISO/IEC 27001/27002:2013
3. ISO 22301
4. PCI DSS

The Data Centre is located within the UK

All client data is located in a single subscription in Microsoft Azure. Data is stored in an SQL database and only accessible by administrators.

Software Development process and methodology

The developer uses a UI first development process enabling the collection of the data required before putting together the data store. SSL is always used for accessing the front-end system, as well as for the development of the API.

Passwords are double hashed when inserting the data into the database so that no-one is able to read any password stored.

The API is built using a token-based system that only remains active for 20 minutes after its last use. Accounts are locked after a specified number of failed attempts.

Applications and interfaces (APIs) are designed, utilising by default, industry standards from OWASP.

SDLC Process

The stages involved in MOT's development are as follows:

- Planning
- Defining
- Designing
- Building
- Testing
- Deployment

The following are included as part of system testing:

- Threat modelling – No
- Peer Code Review – No
- Server Hardening – Yes, we follow Azure best practices
- Vulnerability and Penetration Testing – No

Audit, Assurance and Compliance

It is acceptable for the client to complete audits and security testing of the MedsOnTrack service, providing that at least 1 week's written notice is given.

MedsOnTrack is subject to UK data protection laws and has developed a GDPR framework.

Business Continuity and DR

The service is hosted in Azure UK South data centre and will failover to UK West data centre (which by definition falls within the same jurisdiction) if an issue occurs. By default, data is automatically replicated three times within the primary region, and three times in the paired region.

The service is backed by a Disaster Recovery plan, the maximum tolerable downtime for the service is 15 minutes. The failover zones are restricted to the EU.

Recovery plans will be tested fully within the first year of service.

Incident Response Plan – currently under development

MedsOnTrack confirm that clients will be notified in the event of an incident which affects their information and services.

Change Control

A change control process is in place and includes the following:

- Estimation of the impact of the change
- Authorisation of changes
- Rollback plan & Back out procedures
- Testing of changes

MedsOnTrack
Data Policy

Data Security and lifecycle management

MedsOnTrack acknowledge the level of sensitivity of the data stored and as such have policies in place to reflect this.

Data security at rest, and during transmission

SQL Server encrypts data with a hierarchical encryption and key management infrastructure.

Web based entry points: SSL is used in all connections, external and internal

Clients are responsible for the access security to their devices

Production data is never used for testing purposes

Deletion of client data:

- When a storage account is deleted in Azure the data is permanently removed from the live system
- Backups of the data may exist depending on the archive life cycle
- MedsOnTrack reserve the right to store off-line data for an appropriate period in case of future claims or disputes

Data Centre security

All Microsoft Data Centres are compliant with all relevant certifications, more information can be found here https://azure.microsoft.com/en-gb/overview/trusted-cloud/

Governance and Risk

All configurations are created using Microsoft best practices

MedsOnTrack adopts a continuous process of monitoring and assessing risks associated with services provided to clients. This includes:

- Server security as stated above
- Data held on personal devices

MedsOnTrack
Data Policy

Information Security policies and procedures cover

- Administrative controls over data access
- Technical safeguards for hardware and software
- Safeguards to prevent unauthorized access
- Safeguards to prevent data loss or breaches
- Safeguards to prevent unauthorised alterations or destruction to systems or data

HR

All MedsOnTrack staff are fully vetted

Non-disclosure agreements are in place with third parties with whom information relating to client's data is accessible. The software developers retained by MedsOnTrack are the only third party that this applies to.

Access Control

All users are assigned individual user accounts and passwords

Sharing of passwords is discouraged and needs to be controlled as part of the client's data security policy.

Separation of duties is enforced between developers and administrators

Infrastructure Security

Audit logs are retained for a defined period

Audit Logs are retained by Microsoft Azure according to their policies

Networks are segregated using firewalls

There is an Intrusion Prevention System (IPS) monitoring and blocking potentially malicious threats at the perimeter of critical network zones

Wireless is in use within the organisation:

- Access points are protected by perimeter firewalls configured to restrict unauthorised traffic
- Strong encryption is used for authentication and transmission
- Vendor default settings are changed (Including - encryption keys, passwords, and SNMP community strings
- The software developers have the ability to detect rogue access points

MedsOnTrack
Data Policy

Threat and Vulnerability Management

AV is in place on all systems hosting or potentially hosting client information

Patches (application and OS) are deployed to the production systems regularly

Interoperability

MedsOnTrack do not use 'open and published APIs'

All structured and unstructured data will be made available to the clients and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files), typically via a password protected spreadsheet.

MedsOnTrack have the facility to provide service-to-service application (API) subject to confirmation of data requirements and may be subject to additional cost.

MedsOnTrack use secure (e.g., non-clear text and authenticated) standardised network protocols for the import and export of data and to manage the service.

MedsOnTrack use Microsoft Azure Cloud platform as a service which is built on the Hyper-V 3 technology stack, which is an industry-recognised virtualisation platform and standard virtualisation format.

March 2018

Version 1.02