POL_401	Mapmydiabetes Security Policy	Authorised:

1 INTRODUCTION

Mapmydiabetes (the "**Service**") is a web-based browser application service operated by Mapmyhealth Limited ("**Us**", "**Our**"), a company registered in England and Wales with Registered Number **7989820**.

All of the different forms of data, content, and information described below are collectively referred to as "**information**." Where that data identifies you personally it is "**personal information**", and where personal information relates to your physical or mental health or condition, ethnicity or religion, it is "**sensitive personal information**". Where we process your information to remove personal information, the resulting information is "**anonymised information**".

The protection of your information is of critical importance to us. All aspects of our Service and the associated infrastructure conform to the highest industry standards for storing and handling of information and have been reviewed by independent security consultants.

In summary, our system architecture provides a very strong foundation for security of personal information and sensitive personal information, with a combination of architectural design, strong encryption and service security features designed to help ensure that the system is less vulnerable to common web application security attacks.

2 SCOPE

This Security Policy document covers the security policy for our Service, a patient self-management system built on the MyHealth Engine patient self-management platform.

3 POLICY

SECURE DATA HOUSING

1. The data centre that hosts the Service is ISO/IEC 27001:2005 certified and compliant with the data centre TIER-II+ standard. This means:

    - that the data centre has a system for managing information security and has redundant site infrastructure with expected availability of 99.741%
    - Sensitive personal information (other than name and email address) is encrypted with AES 256-bit.
    - Service scanned for vulnerabilities on regular basis.
    - Service protected by Firewall

USER DATA PROTECTION

2. The protection of personal information is of paramount importance to Mapmyhealth. As such the Service takes the approach of encrypting all personal information with the exception of the user's first name, last name and email using the industry standard AES algorithm (AES is a United States government approved encryption algorithm and is in use by all major banking groups to protect customer information). This method makes it very difficult for an attacker to gain unauthorised access to this information.
3. The Service makes use of a data-key which is used to encrypt each individual user database. This key is generated using a secure random number and then encrypted using the user password and salt, ensuring that the key is unique, encrypted and readable only by the user themselves (or other authorised parties, as described below).
4. A key area of data protection required for any service is ensuring that the passwords used by users will remain secure, even where an attacker has access to the database. Whilst given an unlimited amount of time, any password hashing mechanism can be defeated, the Service makes use of a special type of algorithm to maximize the difficulty that an attacker would have in retrieving passwords from a compromised copy of the database.

5. Each user's sensitive personal information is stored in its own personal encrypted database. This database can only be decrypted by users who have access to that user's shared key. This by default includes the user's healthcare professional. All keys are encrypted. Should anyone gain a physical copy of the keys or individual databases, no data could be extracted without knowledge of a user's passphrase.

USER DATA SHARING

6. As part of the functionality of the Service there is a requirement for other parties to gain access to the user information. This has been designed to ensure that the user is in control of who has access to their information, and that only parties who are specifically granted access by the user will be able to see their information. **The default model of our Service is that users agree to provide their healthcare professional with access to their information.**

GENERAL SERVICE SECURITY FEATURES

7. The Service has a number of features to protect against many of the prevalent security issues faced by web-based browser applications:

a) The Service makes use of a layer of database abstraction which provides protection against SQL Injection attacks by ensuring that all user input is treated as such and cannot disrupt the execution of the query.

b) For services processing sensitive personal information, it is important to ensure that all information is encrypted in transit. The Service enforces the use of SSL and makes use of strong ciphers and perfect forward security where supported by a user's browser. The service SSL certificate is secured with a 2048-bit key, as recommended by the Certificate Authority Browser (CAB) Forum.

c) Sessions are limited to 15 minutes of inactivity before they are terminated, reducing the risk that a user's unattended computer provides unauthorised access to their information. Additionally the Service makes use of a server-side store for user session data. This reduces the risk of data stored within the session (e.g., encryption keys or user personal information) being compromised by an attacker with access to a user's local PC.

d) A common issue with web-based security is users making use of weak, guessable passwords. The Service enforces a password quality requirement on all users ensuring that passwords will be more than 8 characters in length and must contain at least one upper case, one lower case and one numeric character.

e) An area of concern with web-based browser applications can often be sensitive personal information being stored in diagnostic log files. All log files contain only the error message and location that the error occurred. The error message doesn't contain any user data.

5 CHANGES TO SECURITY POLICY

8. We reserve the right to change our Security Policy. Any changes we may make to our Security Policy will be posted on this page and, where appropriate, notified to you by e-mail.