Scope

This document contains the definition of an API to allow creation of client accounts linked to a partner account.

Authentication and request structure

This section contains info on what should be included in the header for API requests on behalf of a partner.

Current version

By default, all requests receive the v1 version of the API. You need to explicitly request this version via the Accept header.

```
Accept: application/vnd.harleytherapyplatform.v1+json
```

User agent required

All API requests MUST include a valid User-Agent header. Requests with no User-Agent header will be rejected. We request that you use your GitHub username, or the name of your application, for the User-Agent header value. This allows us to contact you if there are problems.

Here's an example:

```
User-Agent: Awesome-App
```

cURL sends a valid `User-Agent` header by default. If you provide an invalid `User-Agent` header via cURL (or via an alternative client), you will receive a `403 Forbidden` response.

Schema

All API access is over HTTPS. All data is sent and received as JSON but tagged as a custom Mime type (see above).

Blank fields are included as null instead of being omitted when returned by the API.

All timestamps return in ISO 8601 format (UTC).

```
YYYY-MM-DDTHH:MM:SSZ
```

Authentication

The Partner will be provided with a developer account on the HTP platform. This will provide The Partner with an `auth_id` and `auth_secret`.

All requests will be authenticated using the following headers

```
Authentication: hmac <auth_id>:<hashed_auth>
Date: <iso 8661 date utc>
X-HT-Request-id: <request_id>
```

In the header the variables are as follows:

auth_id is the id assigned in the HTP developer portal

date is the date of the request in the format used for the **hashed_auth** (see below). requests received more than 10 minutes +/- server time will be rejected with HTTP status 401.

request_id is a unique string (e.g. uuid) generated by the client that will not be repeated by the client within a period of 24 hours, all requests with repeated request_id received within 24 hours will be rejected

The HTP servers will maintain a database of request_ids used in the last 24 hours and will respond to a request with a repeated request_id with HTTP status 401

The **hashed_auth** is calculated as follows (ruby):

```
secure_hash = OpenSSL::HMAC.hexdigest('SHA256', <auth_secret>, <data>)
```

Where data is a string constructed as follows:

```
HTTP_METHOD+SPACE+URL+SPACE+REQUEST_ID+SPACE+ISODATE
```

An example for the data string for a GET request for a specific user record would be:

```
"GET /users/123 129d81ec-266c-4a0f-bc9b-9f6ff2b731e1
2018-11-12T09:34:45.124Z"
```

API client ids and secrets will be provided for both production and staging environments. Dates are encoded in exactly the format they are received in the header from The Partner.

The API urls base to be used are as follows:

Clients

Clients are the end users of the HTP system and require an account to allow them to login.

We allow login via email or mobile using a one time passcode so when creating a user account we use both mobile number and email to ensure no duplicate accounts are created.

Creating a client account

When a partner client does not have an existing HTP account (or The Partner does not know whether a client has an HTP account) the following API call will create an account for the client:

```
POST /clients
{
  "partner_client_id": "<unique_id_for_partner_client>",
  "mobile_number": "+447765123456",
  "email": "mail@example.com",
  "first_name": "<first_name>",
  "last_name": "<last_name>",
  "date_of_birth": "DD/MM/YYYY"
}
```

Note at present the First name, Last name and Date of birth are mandatory and clients logging in will be prompted to complete these details - not least because therapists need to know the name and the age of the prospective client.

The responses to the request will be as follows:

- If the request is accepted and the resource has been created or found the following response will be provided:

  ```
  HTTP/1.1 200 Success
  {
    "client_id": <ht_client_id>,
    "handover_url": "<url_with_encoded_client_identity>"
  }
  ```

Get a client login link

In order to obtain a link that can be shared with a client The Partner service should use the following endpoint:

```
GET /clients/<client_id>
```

HTTP responses to this could be

```
HTTP/1.1 404 Not Found # no matching client is found
HTTP/1.1 400 Bad Request # malformed request
HTTP/1.1 401 Unauthorized # authentication is not valid
HTTP/1.1 403 Forbidden # request is valid but no access to resource
HTTP/1.1 200 Success # client found, body contents as follows:
HTTP/1.1 201 Created
{
  "client_id": <ht_client_id>,
  "handover_url": "<url_with_encoded_client_identity>"
}
```

In the case of a 200 response, the URL returned is a URL that may be used by the client to login to the HTP site. It includes an encoded version of the client id.

For security before entering their account, the client will be sent a passcode to their mobile which they will need to enter to proceed to the destination page.

Sample node app

A sample app that uses this API can be viewed here:
https://github.com/harleytherapy/partner-sample-app