FDP EXPANDED CLEARINGHOUSE API USE AGREEMENT - 5/1/2019

This Use Agreement describes the purpose and functions of the Federal Demonstration Partnership (FDP) Expanded Clearinghouse System-to-System Application Programming Interface (API), and the responsibilities and expectations of the Authorized Users of the API.

An Authorized User is any Participating Organization in the FDP Expanded Clearinghouse who requests and is granted access to the API by FDP. Authorized Users agree to adhere to the terms of this agreement in order to maintain access to the API.

Becoming an Authorized User

To become an Authorized User, a Participating Organization must request, and then receive from FDP, an API access token.

The request for token is made via a form accessed on the FDP Expanded Clearinghouse webpage located on the Data Access page.

- Only a member of the Participating Organization with an FDP Expanded Clearinghouse account may log in to access this form.
- The form requires a technical contact name and email address (which do not have to be the same as the user submitting the form).
- Acceptance of this API Use Agreement is required to submit the form.

** Should the FDP elect to expand access to the API at some future date, this document will be updated to reflect any modifications to the process for becoming an Authorized User.

Functions of the FDP Expanded Clearinghouse API

The API:

- Provides read-only access for Authorized Users to Participating Organizations Profile data stored in the FDP Expanded Clearinghouse. Details are provided in the API spec document located at https://app.swaggerhub.com/apis/vumc/fdp_ech.
- Tracks each call to the API, including the authorization token and the IP address of each request.

Requirements of API Authorized Users

Authorized Users of the FDP Expanded Clearinghouse API shall not:

- Make excessive requests to the API
    - The API includes rate limiting or throttling technology to limit the number of requests from an individual user over a finite period of time.
- Share the authorization token with third parties
    - Authorized Users may share their token with their software vendor (as applicable), provided the vendor signs the below certification acknowledging that they may not use the token to provide API access for its other customers.
    - *Knowingly sharing the token is grounds for having your access to the API terminated via disabling of the authorization token and possible removal of the Participating Organization's Profile from the Expanded Clearinghouse.*
- Providing data to third parties
    - Data access is permitted only for the Authorized User and, as applicable, Authorized User's software vendor (for use with Authorized User's instance of vendor's software – see above).
    - Authorized User shall not share the output from the API with any third parties without the consent of the FDP Expanded Clearinghouse Steering Committee.

Abuse of any of these requirements is grounds for termination of API access, and possible removal of the Participating Organization's Profile from the Expanded Clearinghouse, at the discretion of the FDP.

Best Practices

In addition to the above requirements, Authorized Users agree to use best efforts to adhere to the following best practices in their local implementations of the API:

- Local persistent storage of Profile data: Storing the entire profile data set in persistent local storage is strongly discouraged, the FDP recommends retrieving individual profile data on demand (optionally with local caching discussed below).
    - Profile data may change frequently and at non-regular intervals causing concurrency issues and may result in business decisions being made with out-of-date data. The API provides real-time access to a "system-of-record" data source.
    - Should the Authorized User's use case demand (or local system's technology require) storage of the entire data set, FDP expects that the Authorized User will implement a refresh of the entire data set on a frequent basis, no less than once per month and ideally once per week, in order to ensure local system is working with the most current Participating Organization data.
- Local short-term caching: As allowed by Authorized User's local system, local short-term caching of API output (e.g. 5-15 minutes) is strongly recommended to reduce instances of multiple identical calls to the API over short time periods. This minimizes load on the FDP Expanded Clearinghouse servers.

By accessing the API using their authorization token, the Authorized User agrees to all terms and conditions above.

☐ Check here if Authorized User makes use of a Vendor system and will be sharing its API token with said Vendor

Responsibilities of Vendor

Vendor acknowledges by signature below it shall use best efforts to comply with the above terms and conditions, including but not limited to:

1) Use of Authorized User's token in Vendor's system should provide API access only for Authorized User, and that specific token will not be used by Vendor to provide API access to FDP ECH data for any other customers. (Each customer+token combination requires a separate signed instance of this agreement.)

2) Adhere to the Best Practices to the extent feasible and limit excessive traffic over the API.

Name of Vendor: _____

Name of System/Product (if different from Vendor name): _____

Vendor Representative Signature: _____ Date: _____

Print Representative Name: _____