TDRAAP Information and FAQs About UDAP Testing

1. *How do I determine which tests I should take and submit as part of my TDRAAP Program?*

The following decision tree is available to aid in determining which tests are to be successfully passed and submitted within your EHNAC materials (https://test.udap.org/oauth/stage/register):

1. ***Are you seeking accreditation/certification for client, server, identity service or a combination thereof?***
2. ***For which Star Level according to the Glide Path do you wish to achieve?*** (1-5)
3. ***Does your client app support Authorization Code Flow, Client Credentials Code Flow or both?***

RESPONSE:

The applicable tests are as follows based on the responses above. If more than one role or grant type is selected, the Candidate must complete the corresponding tests for each role/grant type combination separately. For example, to accredit a client supporting both Authorization Code and Client Credentials, tests from both A and B (below) need to be completed. See respective charts below.

Additionally, Comprehensive Program participants completing accreditation in 2021 and beyond are able to accredit at a chosen Star Level. The lowest level of compliance is that which is currently required by regulations--OAuth 2.0 Authorization Code grant with Client ID and Secret, evaluated in Test 5. See TDRAAP Glide Path Levels on the EHNAC Website for additional information about Star Levels.

A. Client + Authorization Code Flow - (TDRAAP Basic* or Comprehensive Programs)

Stars	Tests
1	5**
2	5, 3
3	5, 3, 7
4	TBD
5	TBD

* The Basic program is only available to Client-only candidates supporting grant type = Authorization Code (A) for a patient's access to their own data. 1 or 2 stars may be attained.
**The 1-star level is available only to Basic Applicant Clients.

B. Client + Client Credentials Flow - (Comprehensive Program Only)

Stars	Tests
1	N/A
2	3
3	3, 9
4	TBD
5	TBD

C. Server + Authorization Code Flow and Client Credentials Flow- (Comprehensive Program Only)

Stars	Tests
1	TBD
2	16
3	16, 18, 20
4	TBD
5	TBD

It is generally assumed that servers will need to successfully pass both the Authorization Code Flow and the Client Credentials Flow tests. Exceptions may be made based on the business model upon request.

TDRAAP Information and FAQs About UDAP Testing

Additional Examples to Consider When Selecting Basic Certification or Comprehensive full Accreditation.

Specific Examples when TDRAAP Basic Certification is appropriate:

The Basic program is limited to apps accessing data with Authorization Code Flow with a patient's own username and password for accessing or authorizing access to their own data.

1. If the client is solely an aggregator of patient data for the purpose of the patient's own access, Server scope is not necessarily triggered, but is recommended. In this case, the candidate may choose to test Server capabilities and pursue Comprehensive full Accreditation.
2. "Consumer-directed exchange" is a workflow that involves access to health data by someone other than the patient. If the patient's username and password assigned by the health system authorizes such access from the health system as the only workflow supported by the client, only Basic Certification is required.
3. "Consumer-mediated exchange" is a workflow that involves access to health data by someone other than the patient, when data is stored by an intermediary that is not a Covered Entity or is not the Covered Entity from which the health data may have first originated. Client apps enabling consumer-mediated exchange, or other such intermediaries are required to pursue TDRAAP Accreditation including the Server scope.

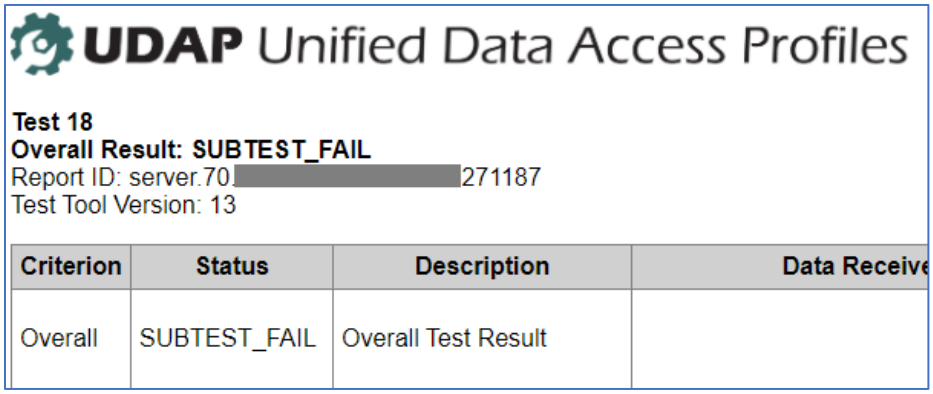
Specific Examples when TDRAAP Comprehensive Accreditation is Required:

1. A broadcast query without the patient's portal credentials requires TDRAAP Accreditation even if the client happens to use authorization code flow for its own access to data.
2. If the Consumer Facing App or an associated service lets the patient also allow access by someone else to the data the client has obtained, TDRAAP Accreditation must be attained and in that case also includes the Server scope. If the client is an aggregator of patient data for purposes beyond the patient's own access, for example, and health data is accessible by third parties, then the TDRAAP Accreditation Program is required.
3. Allowing data to be accessed by others beyond the individual with their own username and password assigned by the responding FHIR server (for example, the patient may authorize an app other than the candidates to access data that is stored by candidate) triggers the full TDRAAP Accreditation Program.
4. Access by someone other than the patient, even in consumer-directed exchange, to data when it is stored by the Candidate requires full TDRAAP Accreditation.
5. If a probabilistic match on the patient's asserted identity attributes is used to make an authorization decision, that is also an example of a scenario requiring TDRAAP Accreditation even though data access may be only one patient at a time, and clients implementing this (and who are either requesting or responding to the match) would also include Identity services in their scope unless relying upon an accredited Identity service for all applicable criteria.
6. If a comprehensive candidate wants to certify both client and server, all relevant tests from the lists above must be passed. At this time, this means a candidate who wants to certify "everything" will have to pass all tests. It is generally expected that servers will need to support both grant types.

TDRAAP Information and FAQs About UDAP Testing

2. ***What if my Client App has multiple versions? Perhaps there is 1 App name referring to the same core functionality, but there is a version of the App for Android, iOS and web browsers … is that 1 or 3 TDRAAP Basic Certifications?***
When multiple versions exist, the underlying software implementing tested workflows varies, or the deployment environment or management practices within a single environment vary, each version must be separately certified. Privacy/Security and/or UDAP testing may have varying results, and this is why 3 TDRAAP applications must be completed, and three responses submitted.

3. ***What does the Report Look Like and How does a Candidate Get it?***
Each submitted report from the Test Tool will show the Test number and Overall Result right at the top. The following must be readable in order to process the Desk Review/full Review: ***"Overall Result: PASS".*** Candidates should save passing reports as they appear on web browsers in PDF format in order to be submitted as evidence to EHNAC. Here is an example cropped from the top of one of the reports:



UDAP Unified Data Access Profiles

Test 18
Overall Result: SUBTEST_FAIL
Report ID: server.70[redacted]271187
Test Tool Version: 13

Criterion	Status	Description	Data Receive
Overall	SUBTEST_FAIL	Overall Test Result	

"Subtest Fail" means at least one of the components of this test did not succeed.

4. ***What is the difference between the EHNAC/UDAP.org TDRAAP program and the certification program recently announced by Drummond and Aegis?***

The two programs are complementary to one another and evaluate different aspects of a FHIR implementation, with minimal overlap between the two. More specifically:

- The EHNAC/UDAP.org program tests capabilities related to privacy and security, including the use of digital certificates and signed tokens, and includes an associated privacy and security assessment that is tailored to client, server and/or identity service capabilities.

- The Drummond/Aegis program tests base FHIR resources for conformance with certain implementation guides. This program is similar to the certification of a system's FHIR data elements corresponding to data in health record systems but with a focus on the CMS Patient Access rule for payers' servers.

5. ***Where do I go if I have questions or feedback about the UDAP Test Tool?***

If you have any questions or issues while using the UDAP Test Tool, or simply want to share your feedback, you may email collaborate@udap.org or click on the "Join the google group" link at the bottom of the UDAP.org website.

TDRAAP Information and FAQs About UDAP Testing

6. How Much Does the Test Tool Cost and What are the Terms of Use for UDAP Testing?

RESPONSE:
Organizations choosing to test their own software with the UDAP Test Tool hosted at UDAP.org will find that the UDAP specifications are free to use and can be implemented by anyone. While there is no cost, using the Test Tool requires each developer to complete a Developer Account registration and agree to the Terms of Use and License Agreement set forth by the organization which administers the and testing tool and provisions complimentary certificates for use with it, EMR Direct.

The following language describes UDAP licensing and is included at the end of each UDAP profile:

> *UDAP.org grants to any interested party a non-exclusive, royalty-free, worldwide right and license to reproduce, publish, distribute and display this [Draft Specification, Working Copy, or Specification], in full and without modification, solely for the purpose of implementing the technology described in this [Draft Specification, Working Copy, or Specification], provided that attribution is made to UDAP.org as the source of the material and that such attribution does not indicate an endorsement by UDAP.org.*

7. What is the difference between technical FHIR ecosystem testing performed under TDRAAP and that done with Inferno by UL, Infoguard and Drummond?

RESPONSE:
Inferno (https://inferno.healthit.gov/) is a **FHIR server** software testing tool which was originally created under ONC guidance as it was designed to verify a server's compliance with aspects of the HL7 FHIR standard, as required to attain 2015 Edition Cures Update health IT certification. Inferno as used by the certification testing labs evaluates different capabilities than the TDRAAP Program. TDRAAP focuses on compliance with the UDAP technical framework (**extensions of OAuth and OpenID for FHIR clients, servers, and Identity Providers** that go beyond health IT certification requirements) and related **privacy and security requirements**.