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://www.udap.org/UDAPTestTool/):

1. ***Are you seeking accreditation/certification for client app, 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. ***If you deploy one or more client apps, do your client app(s) support authorization of the client app via Authorization Code Flow, Client Credentials 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 app 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	Request manual test plan
5	Request manual test plan

* The Basic program is only available to Client app-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 Client apps.

B. Client app + Client Credentials Flow – (Comprehensive Program Only)

Stars	Tests
1	N/A
2	3
3	3, 9
4	Request manual test plan
5	Request manual test plan

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

Stars	Tests
1	N/A
2	16
3	16, 18, 20
4	Request manual test plan
5	Request manual test plan

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.

Additional Examples to Consider When Selecting Basic Certification or Comprehensive 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 or their authorized user's[1] own username and password for accessing or authorizing access to the patient's data.

1. If the Client app is solely an aggregator of patient data for the purpose of the patient's or their authorized user's[2] access, Server scope is not necessarily triggered, but is recommended. In this case, the candidate may choose to test Server capabilities and pursue TDRAAP Comprehensive 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 authenticates the patient who then authorizes such access to their records at a health system by the patient-designated Client app as the only workflow supported by the Client app, only TDRAAP Basic Certification is required of that Client app.
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 and other such intermediaries are required to pursue TDRAAP Comprehensive Accreditation and are required to include the Server scope when patient data is stored by the Candidate for access by someone other than the patient, for example when the patient authenticates to the system to authorize that data be transferred to a third-party Client app.

Examples of when TDRAAP Comprehensive Accreditation is Required:

1. A targeted (to a single endpoint) or broadcast (to a collection of endpoints) query without the patient's or their authorized representative's credentials issued by the health data creator, or an accredited Identity Service they trust, to authenticate the user requires TDRAAP Comprehensive Accreditation by Client apps and Servers deploying this workflow. Client apps to which PII is

[1] Each additional mention of a patient's credentials in this document is similarly intended to mean the credentials of the patient and/or their authorized user(s).

[2] Each additional mention of a patient's access to their data in this document is similarly intended to mean the patient's or their authorized user's access.

returned from an Identity Service, beyond what an individual may explicitly authorize via a screen they view as part of an OAuth flow and about all of which the Client app's privacy policy is readily accessible, are required to scope the management of that Personally Identifiable Information into their TDRAAP accreditation.

2. If the Consumer-Facing App or an associated service lets the patient or their authorized representative also allow access by someone else to the data the Client app has obtained, TDRAAP Comprehensive Accreditation must be attained and in that case also includes the Server scope. If the Client app 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 Comprehensive 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 Candidate's to access data that is stored by Candidate) triggers TDRAAP Comprehensive Accreditation.
4. Access by someone other than the patient or their authorized representative, even in consumer-directed exchange, to data when it is stored by the Candidate requires full TDRAAP Comprehensive Accreditation.
5. If a match on the patient's asserted identity attributes, identifier(s), or other externally-provided metadata is used to make an authentication or authorization decision, that is also an example of a scenario requiring TDRAAP Comprehensive Accreditation even though data access may be only one patient at a time, and Client apps 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 or other trusted UDAP Tiered OAuth workflow for all applicable criteria.
6. "App-Mediated B2B exchange with Patient User" is a workflow in which patient authentication is asserted by a privileged Client app instead of occurring explicitly within the transaction. As with consumer-directed and consumer-mediated exchange, data is released to a non-Covered Entity or the patient themselves. Client apps and Servers deploying this workflow are required to pursue TDRAAP Comprehensive Accreditation for their respective role(s).
7. If a TDRAAP Comprehensive Candidate wants to certify both a Client app and a 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 Authorization Code and Client Credentials grant types. One exception to this is that Candidates who are only assuming the role of Identity Service are not required to perform tests involving UDAP Dynamic Client Registration, since one-off registrations of relying parties to Identity Services are permitted by the UDAP standard, however these tests are recommended.

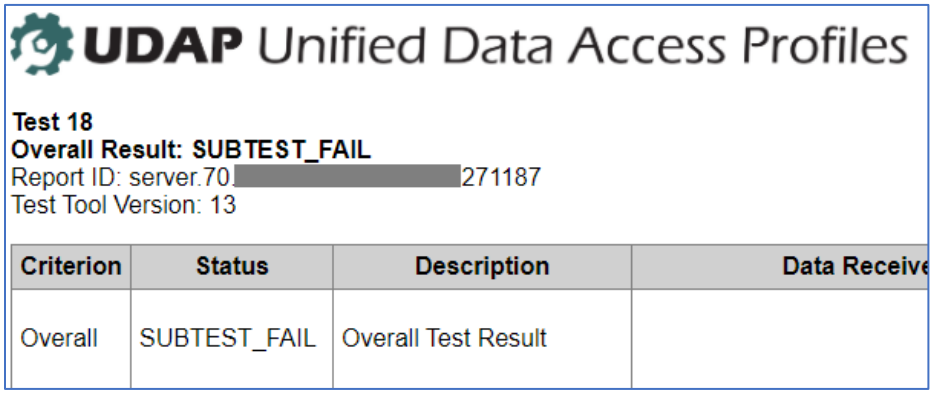
2. ***What if my Client app has multiple versions? Perhaps there is 1 App name referring to the same core functionality, but there is a version of the App for Android, iOS and web browsers … is that 1 or 3 TDRAAP Basic Certifications?***

When multiple versions exist, the underlying software implementing tested workflows varies, or the deployment environment or system 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. ***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 (preferred), where answers to other questions asked by the community are also available.

5. ***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 for a TDRAAP Candidate to use the UDAP Test Tool, using the UDAP Test Tool requires each developer to complete a Developer Account registration and agree to the Terms of Use and License Agreement set forth by EMR Direct, which maintains and hosts the UDAP technical tests and provisions certificates for use with it.

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

> *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.*

The HL7 UDAP Security Implementation Guide includes additional license information.

6. ***What is the difference between technical FHIR ecosystem testing performed under TDRAAP and that done with Inferno by UL (formerly InfoGard), ICSA Labs, SLI, Leidos 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 goes beyond health IT certification requirements and the Inferno tests to focus on compliance with the UDAP technical framework (**extensions of OAuth and OpenID for API ecosystem participants such as FHIR client apps, servers, and Identity Services**) and related **privacy and security requirements**.

7. ***What is the difference between the EHNAC/UDAP.org TDRAAP program and the certification program offered 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, scalability, identity, and security, including the use of trusted digital certificates and signed tokens, and includes an associated privacy and security assessment that is tailored to client app, 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 (see FAQ #6) but with a focus on the CMS Patient Access rule for payers' servers.