Trust is a core component which must be met in order for our industry to safely, securely and efficiently move sensitive data across the healthcare continuum in an interoperable manner. With the 21st Century Cures related regulations, patients are increasingly able to ask for their health information on any app of their choice. With the advent of new technologies, increased awareness and better interoperability, we expect an explosion of the use of these Client Apps.

But first, we must solve a logistics problem – Client App registration today is usually manual. The current process (today's OAuth and OpenID) is simply not going to work in an interoperable world because it cannot be scaled across systems to quickly and safely pass required registration and authentication information once the volume of broad-based consumer demand for health data interoperability increases. That is why automation is needed to scale the process of enabling trust between the growing number of Client Apps, Servers and Users of these systems.

The ability to efficiently register and authenticate endpoints is a core component of interoperability throughout the healthcare information highway. Through the creation of a technical and governance infrastructure, TDRAAP supports interoperability with a specific focus on technical standards enabling trust and transparency for both organizational and individual access to data.

— Lee Barrett, Executive Director and CEO, EHNAC
EHNAC/UDAP.org’s new Trusted Dynamic Registration and Authentication Program provides an answer to the following questions:

As a Health Information Exchange:
*How can you trust the Technical App Developers within the API/FHIR® Ecosystem who are knocking on your door to get access to patient data?*
Answer: If they are TDRAAP Accredited/Certified, you know they have met stringent requirements for privacy/security and UDAP testing and can be trusted to share sensitive information.

As a Technical Application Developer:
*How can you demonstrate you can be trusted to gain access to clinical data within the API/FHIR ecosystem?*
Answer: If your organization attains TDRAAP Accreditation/Certification, you show others you have met stringent requirements for privacy/security and UDAP testing and can be trusted to share sensitive information.

As a Health Plan (Employer Health Plans)/Payer and/or Business Associate:
*How can third parties (not subject to HIPAA) be trusted to appropriately handle data in an interoperable API/FHIR based ecosystem?*
Answer: If third parties present TDRAAP Accreditation/Certification evidence, you know they have met stringent requirements for privacy/security and UDAP testing and can be trusted to share sensitive information.

As a Health System or other Covered Entity:
*How can third parties (including other Covered Entities as well as those not subject to HIPAA) be trusted to make claims about the identity of a user or the subject of a query?*
Answer: If these organizations present TDRAAP Accreditation/Certification evidence, you know they have met best practices and other requirements for identity management and UDAP testing and their identity-related claims can be trusted.

Roadmap for Interoperability – TDRAAP Star Level Glide Path

Designed for healthcare stakeholders, including application developers, healthcare systems and payer organizations, the Glide Path roadmap offers a consistent methodology to be followed by the industry during the collective move from basic OAuth 2.0 use to a more scalable and efficient framework providing advanced security and scalability through reusable client application, server, identity provider and end-user credentials.

The TDRAAP Star Level Glide Path offers levels of authentication on a one- through five-star scale. Organizations are encouraged to start with the current requirements of OAuth 2.0 and advance along the Glide Path incorporating the use of the Unified Data Access Profiles (UDAP), until they ultimately reach the highest level which promotes the broadest scalability, greatest security and the best cost savings for clients, servers, identity services and patients. The Star Level format was developed in response to community feedback to define a method to easily indicate current cross-system capabilities, accelerating secure access to health data across organizational boundaries.

HL7® and FHIR® are registered trademarks of Health Level Seven International and their use does not constitute an endorsement by HL7®.