Containing FHIR Implementation: Threats and Best Practices Evaluated by TDRAAP

Each year, the EHNAC Criteria Committee gathers topics brought to the group as part of its public criteria review process. In 2021, the industry expressed concern about the threat mitigation in implementations of the HL7® FHIR® standard, and this table was developed by EHNAC & UDAP.org to describe how the Trusted Dynamic Registration & Authentication Accreditation Program (including the Privacy/Security review process and policies and procedures along with the technical framework certification) helps to address these important ecosystem management considerations.

The chart on the following pages may be used to inform risk assessment for those handling eHI within the FHIR ecosystem.

Containing FHIR Implementation: Threats and Best Practices Evaluated by TDRAAP

EHNAC UDAP

	Mitigation									
Threat Vector or Recommendation*	Authorization Code, Client ID & Secret	UDAP Trusted DCR	UDAP JWT-Based Authentication	UDAP Certifications & Endorsements	UDAP Server Metadata + Claims Validated by Servers	Claims Validated by Clients	UDAP Tiered OAuth	EHNAC Privacy & Security Assessment	Evaluated by UDAP Test Tool	**Notes**
TDRAAP Glidepath Level	★	★★	★★	★★★★		★★★★★		Varies	Varies	
Incorrect use of encryption, token signing or validation	◉	◉	◉	◉	◉	◉	◉	◉	●	Cryptography is complex to manage and cybersecurity skills are needed to securely scale the API ecosystem
Intercepted network traffic and similar DNS spoofing exploits		◉	◉	◉	◉			◉	◉	Short token lifetimes, system identification and use of trusted certificates reduce this risk in the UDAP framework
Malicious server used to compromise user or client credentials				◉	◉	◉		◉	●	Data provenance is another negative consequence of a bad actor on the server side
Exploitation of systems unable to secure a secret	◉	◉	◉	◉	◉			◉	◉	UDAP framework includes only those systems able to protect a private key, secret or token
Lookalike client app obtains an access token		◉	◉					◉	●	Consumers may mistakenly access an app with similar name and logo; certificates provide endpoint confidence
Malicious client app obtains an authorization token from IdP		◉	◉				◉	●	●	Servers can identify good Basic apps certified at 2+ Stars. Tiered OAuth further addresses via use of back channel

◉ Addressed by indicated mitigation in TDRAAP Basic and Comprehensive Programs

● Addressed by indicated mitigation in TDRAAP Comprehensive Program ONLY

	Mitigation									
Threat Vector or Recommendation*	**Authorization Code, Client ID & Secret**	**UDAP Trusted DCR**	**UDAP JWT-Based Authentication**	**UDAP Certifications & Endorsements**	**UDAP Server Metadata + Claims Validated by Servers**	**Claims Validated by Clients**	**UDAP Tiered OAuth**	**EHNAC Privacy & Security Assessment**	**Evaluated by UDAP Test Tool**	**Notes**
TDRAAP Glidepath Level	★	★★	★★★	★★★★		★★★★★		Varies	Varies	
Intermediary/app exposure of FHIR or other private APIs without controls typically enabled by health systems								◉		EHNAC recognizes this and properly scopes the candidate, then implements appropriately scoped P&S evaluation
Ability to provide community level management of potential bad actors		◉	◉	◉	◉	◉	◉	◉	◉	Trust recognized participants who meet baseline requirements & remove non-compliant systems
Questionable purpose of use or other assertions from various participant endpoints		◉	◉	◉	◉	◉		◉	●	With certificates from trusted issuers & appropriate policies, participants may exchange more confidently
Security by design, including methodology and procedures for code review, change management, and other devops best practices								◉		Cross site forgery and other cyberattacks require mitigation in advance through design that stays ahead of likely threats
Risk management, including overall governance, risk-based decision making methodology and data classification in alignment with business profile must be in place								◉		UDAP FHIR ecosystem paired with third party review enables validated use of best practices in cybersecurity
Regulatory compliance (federal/state laws & standards) may provide Safe Harbor and raises the privacy and security bar to promote third party stakeholder trust								◉		Ongoing compliance activities need to occur to assure changes are incorporated into the candidate organization
Unknown organization or app operator makes a business-to-business request via stolen client secret		◉	◉	◉				◉	●	Apps cannot register or authenticate in the UDAP framework without a JWT signed using a trusted private key

◉ Addressed by indicated mitigation in TDRAAP Basic and Comprehensive Programs

● Addressed by indicated mitigation in TDRAAP Comprehensive Program ONLY

	Mitigation									
Threat Vector or Recommendation*	**Authorization Code, Client ID & Secret**	**UDAP Trusted DCR**	**UDAP JWT-Based Authentication**	**UDAP Certifications & Endorsements**	**UDAP Server Metadata + Claims Validated by Servers**	**Claims Validated by Clients**	**UDAP Tiered OAuth**	**EHNAC Privacy & Security Assessment**	**Evaluated by UDAP Test Tool**	**Notes**
TDRAAP Glidepath Level	★	★★	★★★	★★★★		★★★★		Varies	Varies	
Differentiate between various privileged, business-to-business apps		◉	◉	◉	◉			◉	◉	UDAP Authorization Extension Objects provide a grammar to inform policy engine logic, beyond Client ID
Flawed credential management best practices for client secrets and passwords	◉	◉	◉					◉		Use of UDAP is moving the industry toward eliminating use of client secrets and expanding use of multi factor auth
Lack of industry standard access control for all sensitive data (or flawed implementation)		◉	◉				◉	◉	◉	Authorization servers and the custom policy logic to successfully manage requires high technical sophistication
Information systems and identity management best practices	◉						◉	◉	●	Fewer account details to remember means stronger credentials; digital identity enables reliable patient access
Injection attack		◉	◉		◉			◉		Data validation and sanitization is performed as part of meeting security by design best practices
Server Side Request Forgery					◉	◉		◉	◉	Knowing a client has been identified as trustworthy helps reduce the risk of malfeasance

◉ Addressed by indicated mitigation in TDRAAP Basic and Comprehensive Programs

● Addressed by indicated mitigation in TDRAAP Comprehensive Program ONLY

*This summary reflects the work of a voluntary collaboration including OWASP.org publications and input from FHIR implementers and is deemed accurate, however it should not be considered a complete list.