DirectTrust™

# DirectTrust Comments on RCE Facilitated FHIR IG and TEFCA Certificate Issuance Process

DirectTrust Community Response

Submitted Electronically: November 7, 2022

# 1 DirectTrust's Comments on TEFCA Facilitated FHIR Implementation Guide – General Trust Questions

## 1.1 Feedback regarding: *The RCE is seeking feedback specifically regarding concerns with managing the volume of certificates needed to operationalize Facilitated FHIR at scale.* ***Do you anticipate that your organization will leverage Facilitated FHIR or wait for an approach Brokering FHIR through a single QHIN Gateway?***

The DirectTrust community is ready to support FHIR in a nationwide and scalable way. Our trust framework is not an exchange Participant in query exchange, but we believe we have an important role to play in supporting technical trust in Facilitated FHIR as well as FHIR brokered through a gateway intermediary. Please see: "*Additional Feedback and Considerations*' for background that may be used to contextualize and contrast DirectTrust's feedback with that of the current Query Based Data Exchange (QBDE) environment.

## 1.2 Feedback regarding: *Approaches that are being considered would place the management of certificates on each QHIN by either requiring each QHIN maintain their own Certificate Authority (CA), or alternatively have an agreement with one CA from an approved list.* ***What risks/concerns are there with either approach?***

The policies of technical trust embodied in a Certificate Policy adapted for the healthcare information exchange environment is essential. There have been several examples of CA compromises over the past decades and in every case, the attack occurred due to untrustworthy operational controls employed by the CA that range from improper procedures used for enrollment, to weak cybersecurity controls, to technology stacks that don't conform to industry standards. Prior history of CA compromises plainly shows that people and processes are consistently the weakest link of running a CA. Cybersecurity experts have also championed the point that humans are the weakest link in any system. The only way to limit exposure to this risk is to ensure carefully crafted processes are followed by the staff who are responsible for adhering to published Policies and carrying out those processes. Ensuring processes are followed is the ultimate purpose and goal of periodically renewed accreditation. This is the foundation on which trust is built and grows.

The value of governance policies and accreditation is exemplified by the risk assessment process undertaken to inform the initial DirectTrust Policies that govern the trust framework. This methodology includes examining risks to PHI, prescribing levels of assurance and certificate distribution methodologies, and evaluating operational controls that are evaluated as part of accredited members' biannual audit processes. The option of having intermediaries issue their own certificates is explicitly prohibited unless they are accredited as an RA/CA.

To support interoperability across CAs, QHINs, and FHIR Servers, a set of certificate profiles that can be easily adjusted to accommodate new requirements from the RCE would be recommended. Also, it is best practice to establish an authority to oversee the addition and removal of Trust Anchors from a Trust Bundle, inspecting certificates in an automated fashion to ensure that a CA's certificates conform to the published Certificate Profiles. Such an approach is maintained today within DirectTrust and enables relying parties throughout the network to trust the Trust Framework and accredited CAs by downloading the Trust Bundle while observing interoperability across accredited CAs. It's worth noting that a Trust Bundle, Root CA, or other trust mechanisms each have differential benefits and drawbacks, however, any approach will require a well-documented process to help the many thousands of actors to trust the infrastructure in a way that is secure, scalable, and easy.

## 1.3 Feedback regarding: *Are there other approaches that should be considered?*

One approach that should be considered would allow QHINs and/or participants to choose to partner with one or more DirectTrust accredited CAs or elect to instantiate a DirectTrust accredited CA themselves.

1) DirectTrust **strongly urges** the RCE to require any CA serving the TEFCA community be accredited, whether they are QHINs, QHIN participants, or commercial CAs. This enables a predictable and reliable level of trust across the environment.
2) Accreditation must include the processes necessary to scale the identity proofing and domain validation components of the certificate onboarding process. As an example, DirectTrust infrastructure scales as well as it does partly because of language in subscriber agreements between CAs and their customers which allow for authorized representatives of an organization to request multiple certificates for itself or its own sub-customers, of which that sponsor is also an authorized representative. Trusted agents take responsibility for verifying the identity of individuals and sometimes organizations. The subject of the certificate must also be able to demonstrate "control" of the domain where the certificate will be installed through a process that is defined within a Certificate Policy and is often automated using standard protocols. Some of the likely participants in the TEFCA ecosystem, such as EHR companies, are among the accredited CAs that issue these certificates for themselves. Others may depend upon the Accredited CAs that offer commercial Certificate issuance services. In DirectTrust, a total of 11 accredited Certificate Authorities serve approximately 300,000 healthcare organizations today. We anticipate more Certificate Authorities than the two currently issuing certificates to Sequoia Initiatives participants will be required to scale FHIR and that a more "commercial" (and even semi-

automated) approach will be required to support the scale. A scalable alternative to Trusted Agents includes advancements in unsupervised remote identity proofing (defined in NIST SP 800-63A) which supports IAL2, a technology currently employed by members of the community.

3) A final point to consider for scale is **automating or semi-automating authorization**. An organization may be legitimately identity proofed at IAL2 with verified control over their domain, but not authorized by a QHIN or Participant to participate in TEFCA. Scaling the authorization of FHIR certificates is outlined in the next section *"How would your organization expect to handle certificates, and how can we scale certificate trust chains and issuance of potentially tens of thousands or more certificates across all QHINs, Participants, and Subparticipants?"*

Observing these three points will enable FHIR to scale while ensuring processes are carefully followed as part of a Trust Framework with Policies that support healthcare. In this approach, the QHINs and Participants would assume a similar role as DirectTrust currently serves for Carequality, as summarized in "Additional Feedback and Considerations."

DirectTrust has proven past performance maintaining multiple trust communication mechanisms including a Trust Bundle, a Root CA, and a Bridge CA. DirectTrust would be pleased to collaborate with the RCE to develop a strategy for managing scalable trust across healthcare FHIR endpoints.

## 1.4 Feedback regarding: *How would your organization expect to handle certificates, and how can we scale certificate trust chains and issuance of potentially tens of thousands or more certificates across all QHINs, Participants, and Subparticipants?*

For an approach to scale trust in identity proofing and domain validation, please see the feedback regarding: *"Are there other approaches that should be considered?"*

This section contemplates scaling trust in authorization. Since new actors seeking certificates to operate in the ecosystem as a part of onboarding will not yet be in the RCE directory, the directory cannot be used by RAs/CAs as a mechanism to determine whether an actor is authorized, but may be relied upon by initiating and responding actors.

A TEFCA environment that supports FHIR will require **at least three hierarchical layers of authorization** that CAs must observe. The unique and complex nature of the TEFCA environment is the precise reason a Trust Framework that is purpose-built for healthcare must be employed as opposed to CAs supporting public web-browsers. These layers of authorization should not be conflated with the identity of the actor or ownership of the domain contained in the certificate. It is conceivable that a certificate could be issued to a healthcare organization that is not authorized to participate in TEFCA, unless a trustworthy authorization process that scales is instituted. The CAs currently supporting the Carequality environment are orders of magnitude away from their capacity to issue certificates due to inefficiencies. The principal inefficiency in the Carequality certificate issuance process is a lack of automation surrounding authorization. The recommendation below aims to address the concern of authorization in an automated and scalable manner.

**The first layer of authorization** communicates which QHINs have been authorized by the RCE. The RCE might elect to publish a list of authorized QHINs that CAs must observe before issuing certificates to, or on behalf of, a QHIN. Another option is for QHINs to provide a document signed by the RCE to an accredited CA during certificate issuance as a means of conveying authorization, among other approaches. Optionally, the RCE could make provisions in its published certificate profile for FHIR certificates to include the URL of the RCE directory or list of QHINs authorized by the RCE in an effort to allow Initiating and Responding Actors the ability to validate that a QHIN was authorized by the RCE.

**The second layer of authorization** occurs at the QHIN level. At this authorization level, the CA must only issue certificates to Participants that have been authorized by a QHIN. The QHIN would serve as the authority that determines eligibility for a Participant to receive a certificate. CAs would not be allowed to issue certificates to parties that were not directly authorized by a QHIN. As an approach to ensure unauthorized certificates are not issued, the QHIN could be responsible for approving/submitting applications to their contracted RA/CA(s) using a process established between the RA/CA and the QHIN that complies with the Certificate Policy. If a Participant wishes to contract with an accredited CA separately (different from the QHIN's CA), the Participant's CA would need to confirm authorization either by documents signed by a recognized QHIN or some other process before issuing the certificate to Participants. The RCE may also require the QHIN to publish a private list of authorized Participants to allow responding actors the ability to validate, in real time, that the subject of the certificate (Participant) was authorized by a legitimate QHIN. Optionally, the RCE could make provisions in its published Certificate Profile for FHIR certificates to include the URL to RCE's directory. Initiating and Responding Actors could use the directory to validate that the Participant was authorized by a legitimate QHIN recognized by the RCE.

**The third layer of authorization** occurs at the Participant level. Some Participants will not have Subparticipants, however, others will. One such example of this third layer in action is EHR vendors who wish to credential each of their customers rather than assume responsibility for their FHIR endpoint. As such, CAs will not be allowed to issue certificates to Subparticipants that were not directly authorized by a Participant that has been listed by a recognized QHIN. As an approach to ensure unauthorized certificates are not issued, the QHIN could be responsible for approving/submitting applications sent to their contracted CA(s) on behalf of Participants using an automated process established between the CA, the QHIN, and the QHIN's Participants that complies with the Certificate Policy. If a Subparticipant wishes to contract with an accredited CA separately (different from the QHIN's or Participant's CA), the Subparticipant's CA would need to confirm authorization either by a documents signed by a recognized Participant or some other process before issuing the certificate to Subparticipants. Optionally, the RCE may also require each Participant that manages Subparticipants to publish a private list of authorized Subparticipants' domains. Initiating and Responding Actors could use the directory to validate that the Subparticipant was authorized by a legitimate Participant recognized by the RCE.

The RCE's directory could consume the private lists of QHINs and Participants to maintain up-to-date information in the directory about the authorized actors participating in TEFCA. **A simple mechanism for authorized personnel to communicate updates** to the directory could also be employed.

Observing these authorization layers ensures certificates are only issued to authorized actors. These authorization layers represent real business relationships and afford the flexibility to allow actors to outsource both the Registration Authority and Certificate Authority functions, or elect to become an accredited RA and/or CA, at their discretion to support scale and demand.

# 2 Role Requirements

General Comments on Section 2

DirectTrust believes that Credential Service Providers (CSPs) are a concept and a role that is necessary to adequately fulfill the goals of Individual Access Services (IAS). Please see our feedback in the section 5.2.6 Individual Access Services

# 3 General Requirements

No Comments on this section.

# 4 Use Cases/Workflows

No comments for this section.

# 5 Infrastructure

### General Comments on Section 5:

DirectTrust's comments in section 1 of this response are largely reflected in our suggested edits outlined below.

### Comments on Section 5.2: Authentication/Trust

**Text:** *"X.509 certificates establish the authenticity of Actors implementing this IG. The RCE will issue one "Intermediate" certificate to each QHIN to seed the QHIN's Certificate Authority. A QHIN's Certificate Authority issues certificates to downstream Actors. Certificates used by any Actor SHALL be chained to the RCE "root" certificate."*

DirectTrust's alternative recommendation: *"X.509 certificates establish the authenticity of Actors implementing this IG. QHINs or participants shall engage in a contract agreement with one or more of the accredited CAs listed by the RCE. Alternatively, a QHIN or Participant may elect to instantiate their own accredited CA. A QHIN's or Participant's Certificate Authority issues certificates for downstream Actors. Certificates used by any Actor SHALL be bound to a Trust mechanism specified by the RCE."*

For more information, please see feedback regarding: *"Are there other approaches that should be considered?"* and *"How would your organization expect to handle certificates, and how can we scale certificate trust chains and issuance of potentially tens of thousands or more certificates across all QHINs, Participants, and Sub-participants?"*

*Broken Links Noted*

We also note that links in the draft to FHIR Security IG references are broken and cannot be reviewed easily. We presume the references are meant to be to the following IG as the reference numbers align with the structure of the IG at the following link and not the normative FHIR Security IG - *https://build.fhir.org/ig/HL7/fhir-udap-security-ig/*

### Comments on Section 5.2.3 – Client Registration

We agree with the inclusion of Dynamic Client Registration as a scalable and automated approach to scale the FHIR ecosystem, both for Business to Business connections and for the IAS use case.

### Comments on Section 5.2.4 – Authorization Code Grant Type (3-leggedOAuth 2.0)

We note that UDAP Tiered OAuth is included in this draft. We applaud the inclusion as we strongly believe reusable consumer credentials will substantially improve the value of IAS to patients and their representatives. For this reason, we strongly encourage the RCE to upgrade support for UDAP Tiered OAuth from an optional/MAY requirement to a MUST (or at least to a SHOULD) requirement with some timeline for mandatory support.

### Comments on Section 5.2.6 - Individual Access Services (IAS) Requests

While the User Authorization Extension Object is stipulated and important information about the requestor is present in the Object, we also think it is important to note "ial_vetted" attributes as a part of this structure need to be reliably protected to determine that an accredited IdP/CSP that was the source of such data is signing the assertion. More than policy is required to ensure that the app was not able to make changes to these verified demographic attributes. We believe accreditation/independent certification to ensure the IdP/CSP conforms to the policies of a technical trust framework should be a requirement to issue credentials for use for IAS. As noted in Appendix B below, the NIST definition of a CSP includes not just IAL assurance, but AAL and credential management requirements as well.

# 6 Appendix A

General Comments for Appendix A: Access Consent Policy OIDs

The RCE might also consider more human-readable URIs if the OIDs are expected to reside within a JWT data structure.

Additionally, there appears to be a conflation between an assurance level and a means of communicating consent. Many of the OIDs in Appendix A also appear in Appendix B. Consent and assurance levels are often used in combination, however, they are not the same and should be communicated differently. DirectTrust recommends more human-readable means of conveying the types of consent to aid a responder in potential manual processing of a portion of requests.

# 7 Appendix B

General Comments for Appendix B: Assurance Levels

DirectTrust observes that Authenticator Assurance Levels (AAL) are absent from this list. In scenarios where an IAS app identity proofs a patient at IAL2, DirectTrust strongly believes the app should authenticate the patient at AAL2 or higher as required by NIST SP 800-63B. DirectTrust recommends adding AAL2 and AAL3 to the list of recognized assurance levels.

# 8 Additional Feedback and Considerations

## Summary

The TEFCA FHIR Implementation Guide proposes a model for technical trust which we feel will not provide adequate security for healthcare data exchange.  We suggest an alternate model that both scales securely and enforces best practices by leveraging DirectTrust as an existing Trust Framework that supports both Direct Secure Messaging and query-based data exchange (QBDE) for all healthcare information exchange.

DirectTrust and our community of certified Certificate Authorities (CAs) have been serving Carequality for nearly two years.  We've proven our community can provide digital certificates for the TEFCA FHIR ecosystem through our accredited Registration and Certificate Authorities utilizing our current Trust Framework. We recognize the scale required by the FHIR ecosystem will require us to refine the current process utilized for QBDE.  We recommend the RCE leverage the DirectTrust Trust Framework and governance to support QHINs in their certificate registration and issuance processes, rather than build a new infrastructure with new policies, new governance, and new CAs operated by QHINs.

## Background

Historically, Carequality and eHealth Exchange managed much of the process of issuing certificates to implementers and participants internally and ensured that only community members received certificates. A single Certificate Authority played the role of issuing the TLS certificates that secured communication among all parties.  Each Participant needing a certificate would be introduced to the CA in a warm hand-off by email.

In 2020, Sequoia and DirectTrust signed an agreement where multiple CAs could service the needs of the Carequality and eHealth Exchange communities with DirectTrust playing a certificate policy enforcement and accreditation role. DirectTrust also coordinated the hand-off process and technical support, which are duties that DirectTrust doesn't typically take on in other environments due to the propensity of these activities to cause a bottleneck. The rationale underpinning DirectTrust's current role in support of Carequality was to maintain as similar a process as possible to what was previously being carried out by Carequality. The hand-off process between Sequoia and DirectTrust remains the mechanism by which the subscribing organization's participation with one of the initiatives is verified. DirectTrust then introduces the subscribing organization's representative to the CA that then takes the process to its completion. The sub-contracted CAs do most of the typical commercial Registration Authority and Certificate Authority activities for the issuance of certificates, including but not limited to: *ensuring the individual identity of the subscriber (at NIST IAL2)*, *ensuring that the organization is licensed to operate in its jurisdiction*, *ensuring that the subscriber has control of the domain/machine where the certificate will be installed*.

In 2021, all the certificates that had been issued by Carequality's previous CA were transitioned to the new DirectTrust-enabled model.

Since Query Based Data Exchange (QBDE) is secured between IHE Document repository gateways using TLS certificates, the total number of certificates required for this model is relatively small. For example, CommonWell Health Alliance is a Carequality Implementer with many participants and thousands of sub-participants, but only one certificate is used to secure the connection between CommonWell as broker and the other Carequality implementers. Some implementers stand up separate gateways and certificates for all their sub-participants, but most do not. This approach has scaled reasonably well for the number of certificates and participants required.

Within the IHE profiles there is an additional security mechanism beyond TLS certificates. TLS is supplemented by SAML assertions that communicate organizational identity through initiating and responding gateways from the sender to the receiver. These two mechanisms together are thought to establish adequate technical trust in the current environment and this model has had broad adoption.

## Serving Business to Business Query Utilizing RESTful Exchange via FHIR

As Carequality, and by extension the RCE and TEFCA deploy FHIR at scale, there will be several substantial changes from the IHE model. First, most FHIR transactions will be communicated without gateways or brokers, thus initiators will need to perform authentication and authorization directly with receivers. The technical means to accomplish this is different under FHIR and these differences change the security and technical trust landscape in a substantial way. Rather than SAML, FHIR transactions will utilize TLS, OpenID Connect (OIDC) and OAuth 2.0 to communicate identity assurance via digital certificates. Rather than relatively few gateway connections needing to be established, these "broker-less" connections will be made between the thousands of FHIR endpoints to communicate trust and information exchange bidirectionally. This ecosystem is not only large, but also dynamic. A Participant of an implementer, or of a QHIN under TEFCA, will be onboarding new Subparticipant healthcare organizations constantly and need the flexibility to onboard these organizations and Users with minimum friction.

It is precisely the scale of this ecosystem that makes reliable credentials for connections so important. Several trust infrastructures have demonstrated such ecosystems at scale successfully, including The International Civil Aviation Organisation (ICAO) supporting international passports, the CA/Browser Forum (CA/B) supporting the internet, the electronic Identification, Authentication and trust Services (eIDAS) supporting trust across EU nation states, and the Federal PKI.  All of these groups ensure that organizations who issue end-entity certificates are accredited and impose strict governance policies to ensure interoperability at scale among all participants.