Carequality Consumer-Facing App Certification Profile

Understandable data use disclosure for healthcare apps

Forward

In the future, the Carequality ecosystem may be commonly used to enable a patient to provide her healthcare data to an app of her choosing. When a patient chooses to share this data, an informed decision about the risks and benefits is sometimes difficult. The Carequality consumer-facing app certification enables health app developers to clearly convey information about the app and their privacy policies for display to a patient to encourage transparency and help consumers make informed choices when selecting products.

The Carequality consumer-facing app certification may be included together with a UDAP "software statement" during trusted dynamic registration of an app with an authorizations server.
This certification does not substitute for more comprehensive and detailed privacy policies.

Carequality Software Statement Extension

During dynamic registration, per the Carequality FHIR Implementation Guide, a requestor presents a Software Statement JWT containing technical information about the requestor. Optionally, alongside this Software Statement, the requestor may also present a UDAP certification. The Carequality Consumer-Facing App Certification is a self-signed certification generated by the application operator. The full certification JWT profile can be found below.

To conform to the Carequality Consumer-Facing App Certification Profile, an additional claim is added to the certification JWT containing a Carequality Patient Disclosure Registration Extension object, as defined below. This extension claim optionally conveys additional information about the requestor which may be presented to the consumer, by the responder when the consumer authorizes the requester to access their data.

This profile enables the requestor to provide information about the app -- specifically: any BAAs with health systems, its funding, a simple representation of its data use, access and retention policies and a few key abilities of the consumer to see and manage their data following authorization. This information is by no means a comprehensive or legal representation of the requester’s privacy or data use policy or any other legal document. This certification does not substitute for more comprehensive and detailed privacy policies; it is merely intended to enable a simple and understandable data use disclosure for

healthcare apps. Further, a requestor technically (but not usefully) complies with this optional profile by asserting no information about their app other than the version of this profile in use.

While this profile does not require any information to be submitted, misleading or inaccurate information submitted as part of this certification profile is grounds for permanent revocation of the app and requestor by the registration authorization server.

The certification JWT headers and claims MUST conform to the requirements in the following tables. Note that generally, although not required, the header values will be the same as those used in the application's signed software statement.

Certification JWT Header Values		
alg	required	The JWA algorithm (e.g., `RS256`, `EC256`, `EC384`) used for signing the registration JWT. All implementations SHALL support RS256.
x5c	required	Contains the X.509 public key certificate or certificate chain [RFC5280] corresponding to the key used to digitally sign the JWS. Each string in the array is a base64-encoded DER PKIX certificate value, with the key used to sign the JWS being first. See https://tools.ietf.org/html/rfc7515#section-4.1.6[IV1]

Certification JWT Claims		
iss	required	Issuer of the JWT -- unique identifying client URI. This MUST match the value of a uniformResourceIdentifier entry in the Subject Alternative Name extension of the client's certificate and MUST match the value of the 'iss' claim of the software statement with which this Certification is submitted.
sub	required	Same as 'iss'.
exp	required	Expiration time integer for this software statementauthentication JWT, expressed in seconds since the "Epoch" (1970-01-01T00:00:00Z UTC). The expiration of the software statement does not negate the patientDisclosure information, defined below. A requestor may update its patientDisclosure information by re-registering.
iat	required	Issued time integer for this software statementauthentication JWT, expressed in seconds since the "Epoch".

jti	required	A nonce string value that uniquely identifies this software statementauthentication JWT. This value SHALL NOT be reused by the client app in another software statement, certification JWT, or authentication JWT before the time specified in the “exp” claim has passed.
certification_name	required	Fixed value: string “Carequality Consumer-Facing App Certification Profile”
certification_uris	required	Fixed value: array with single element: [TBD, e.g. “https://wiki.carequality.org/udap/profiles/consumer-facing-app-certification”]
contacts	required	Array containing one URI string with mailto scheme and a valid email address where the Authorization Server may contact the application operator.
grant_types	required	Fixed value: array containing one string “authorization_code”. Note: This profile is intended for consumer-facing apps using the authorization_code flow.
extensions	required	A JSON Object containing the key "patientDisclosure" with a value conforming to the Carequality Patient Disclosure Registration Extension object requirements defined below.

Example Carequality Consumer-Facing App Certification JWT

Example certification JWT, containing the profiled custom claim, prior to Base64URL encoding and signature (non-normative):


```
{
 "alg": "RS256",
 "x5c": ["MIEE8DCCA.....remainder omitted for brevity"]
}.{
 "iss": "http://appdeveloper.example.com/apps/superapp/v1",
 "sub": "http://appdeveloper.example.com/apps/superapp/v1",
 "iat": 1525209077,
 "exp": 1525209377,
 "jti": "random-jti-generated-by-client"
 "certification_name": "Carequality Consumer-Facing App Certification Profile",
 "certification_uris": ["https://wiki.carequality.org/TBD"],
 "contacts": ["mailto:support@example.com"],
 "grant_types": ["authorization_code"],
 “patientDisclosure”: {
        "version": “1”,
        "company": “My Company”,
        "baas": [{
                "npi": "<provider org my app has a signed BAA with>"
        }],
        "funding": {
                "usersHealthcareProvider": true,
        },
        "dataStorage": “onlyUserDevice ",
        "dataStorageLength": {
                "noDataIsStored": true
        },
        "canUserDeleteTheirData": “all”,
        "doesAppUninstallationDeleteData": true,
        "whoHasAccess": {
                "noOne": true,
        },
        "dataAccessNotification": "userAuthorizedOfEachAccess",
        "userCanAccessTheirData": "complete",
        "otherUsesOfData": {
                "noOtherUses": true
        },
        "seeAccess": "complete"
  }
}
```

Carequality Patient Disclosure Registration Extension object

Carequality Patient Disclosure Registration Extension object **Extension Claim Name: “patientDisclosure”**		
version	required	Fixed value: 1
company	optional	Human readable organization name, e.g. “ABC Hospital”
companyType	optional	String from defined value set. Describes the company offering the app. healthcareProvider | governmentAgency | nonprofit | for-profit | individual
funding	optional	Object explaining of how the app is funded. See funding, below.
dataStorage	optional	String from defined value set. Identifies where the patient’s data is stored through one of the following values: onlyUsersDevice | serversInTheUnitedStates | serversOutsideTheUnitedStates | noDataStorage noDataStorage should be used when data is not retained when the app is not in use.
dataStorageLength	optional	Object identifying the length of time data are retained. See Data Storage Length, below.

canUserDeleteTheirData	optional	String from defined value set. Identifies if user is capable of deleting their data from the app, e.g.: all | some | none “all” should be used if all of a patients data can be deleted from the app by the user. “none” if none of the patients data can be deleted from the app by the user.
doesAppUninstallationDeleteData	Optional	Boolean. True if all data about the user is deleted after a user deleted the app and closes their account.
whoHasAccess	Optional	Object. Identifies who has access to data other than the user. See Who Has Access, below.
userApprovesAccess	optional	String from defined value set. Identifies if a user approves sharing data. userApprovesEachAccess | userApprovesEachEntity | userApprovesPolicy | noUserApproval
dataAccessNotification	Optional	Boolean. True if a user is notified when their data is accessed by someone else.
userCanAccessTheirData	Optional	String from defined value set. Identifies if the user is able to access their own data. complete | partial | none
otherUsesOfData	Optional	Object. Identifies how the app developer uses data about the user, other than providing direct service to the user. See Other Uses of Data, below.
otherUsersData	Optional	String from defined value set. Identifies other individuals from the user’s health record the app uses data about, for reasons

		other than providing direct services to the user. noOne | careTeam | family | proxy
userCanSeeAccess	Optional	String from defined value set. Identifies if the user is able to obtain a record of who has accessed data about them. complete | partial | none “complete” should be used if the app allows users to obtain a complete record of who has accessed data about them. “none” if the app does not allow users to obtain a record of who has accessed data about them.

Funding

Identifies the source(s) of funding of the requestor’s app.

usersHealthcareProvider	Optional	Boolean. True if the app is funded entirely or partly by the user’s healthcare provider.
anotherHealthcareProvider	Optional	Boolean. True if the app is funded entirely or partly by a healthcare provider other than the provider acting as the responder.
purchasesSubscriptionsOrDonations	Optional	Boolean. True if the app is funded entirely or partly by purchases, subscriptions, or donations.
advertisements	optional	Boolean. True if the app is funded entirely or partly by advertisements

saleOfData	Optional	Boolean. True if the app is funded by the sale of data or data access to other organizations
appsOtherBusinessVentures	Optional	Boolean. True if the app is funded by your other business ventures
debt	Optional	Boolean. True if the app is funded by debt or venture capital in a startup company
volunteer	Optional	Boolean. True if the app is produced by volunteers or is available in the open source community
grants	Optional	Array of objects identifying the grant-providing organizations funding the app.

Data Storage Length

Identifies the length of time a patient data is retained.

noDataIsStored	Optional	Boolean. True if the app does not retain patient data following use of the app.
dataIsStoredIndefinitely	Optional	Boolean. True if the app stores patient data indefinitely.
dataIsStoredFor	Optional	Number of seconds which app stores patient data.

Who Has Access

Identifies who has access to user data, other than the user.

noOne	Optional	Boolean. True if no one other than the user has access to user's data. For example, data never leaves the user's device.
appEmployees	Optional	Boolean. True if the app developer's staff have access to user data.
peopleAuthorizedByUser	Optional	Boolean. True if people and groups authorized by the user have access to user's data.
appsAuthorizedByUser	Optional	Boolean. True if apps authorized by the user have access to user's data.
usersCareTeam	Optional	Boolean. True if the user's or patient's care team has access to user's data.
researchers	Optional	Boolean. True if researchers have access to user's data.
appPartnersAffiliates	Optional	Boolean. True if partners or affiliates of the app developer have access to user's data.
government	Optional	Boolean. True if government employees or agencies have access to user's data.
other	Optional	String. Describes others who have access to user's data in simple, understandable language.

Other Uses of Data

Other than providing direct service to the user, how does the app developer use data about the user?

noOtherUses	Optional	Boolean. True if the app developer doesn't use data about the user beyond providing services to the user.
improveApp		Boolean. True if the app may use data about users to improve its services in the future.
research		Boolean. True if the app may user data about users for research.
advertisements		Boolean. True if the app may use data about users for advertising to users.
3rdPartyAdvertisement		Boolean. True if the app may use data about users to allow third parties to advertise to users.
advertisingToOthers		Boolean. True if the app may use data about users for advertising to others.
3rdPartyDirect		String from defined value set. provide | distribute | sell
3rdPartyOther		Boolean. True if the app may provide, distribute, or sell data about users to other parties or applications

3rdPartyDeIdentified		Boolean. True if the app may sell aggregate, generalized, or de-identified data to third parties

References

- https://github.com/smart-on-fhir/smart-on-fhir.github.io/wiki/Dynamic-Client-Registration
- http://www.udap.org/udap-dynamic-client-registration.html
- http://www.udap.org/udap-certifications-and-endorsements.html
- https://tools.ietf.org/html/rfc7591#section-2.2