# Carequality Framework Policies

Version 3.0

May 12, 2025

# Table of Contents

# 1.0 Introduction

The purpose of this document is to establish overarching policies that exist within the Carequality Framework, but outside of specific Use Case Implementation Guides, the Carequality Connected Agreement (CCA), or other Carequality Elements. The policy requirements in this document apply broadly across the entire Carequality Framework. More specific policies defined for an individual Use Case take precedent over the general policies contained in this document to the extent it is not possible to comply with both.

## 1.1. Creating and Updating Carequality Elements

To the extent that a Carequality Element governs current Production activity, and except in cases of non-substantive changes, as defined in Section 1.2 below, Carequality will provide notice of any proposed amendment, including creation of new Elements and/or updates to existing Elements to all Implementers at least sixty (60) calendar days prior to the proposed effective date. Carequality will accept feedback on the draft from all Implementers for twenty-one (21) calendar days, and will provide final text of Element to all Implementers no later than thirty (30) calendar days prior to the effective date. Any Implementer allowed to participate in the Carequality Element's Objection Period, as outlined in Section 1.3 below, shall have thirty (30) days from the date of the publication of the final text to advise Carequality in writing if the Implementer objects to the proposed amendment and the specific reasons for its objection. If more than one-third (1/3) of all Implementers who are eligible to participate in an Objection Period, per Section 1.3 below, object to the proposed amendment, then the amendment shall not go into effect. Otherwise, the amendment shall be effective at the end of the sixty (60) day notice period. Specific timelines for compliance with, and enforcement of new requirements will be defined within the newly created or updated Carequality Element.

## 1.2. Non-Substantive Changes

As defined in Section 3 of the CCA, the development, maintenance, and amendment of Carequality Elements and Policies are under the authority of the Carequality Steering Committee. At its discretion, changes to a Carequality Element that are deemed to be non-substantive may be approved for publication by a vote of the Steering Committee without requiring complete Implementer feedback or an objection period. A non-substantive change may include minor modifications to words, grammar, punctuation, references to other document sections, organization, or other formatting that do not materially change the meaning of the text; changes to internal processes that do not require changes from Implementers; clarification of existing language as it was intended to be understood; and other modifications as determined by the Steering Committee.

## 1.3. Objection Periods

When an objection period is held for a Carequality Element, an Implementer is eligible to participate in the objection period only if the Carequality Element governs a Use Case in which the Implementer has been recognized, as detailed in Section 2 of the CCA. For objection periods to any Carequality Element not specific to any one Use Case, objections will only be counted from any

recognized Implementer of the Use Cases impacted by the change. An Implementer may only submit an objection if they are in good standing with respect to all requirements of the CCA.

A Carequality Element that governs a single Use Case, in which there are no recognized Implementers, will not have an objection period.

## 2.0 Roles

The concept of a role within a Use Case is central to that particular Implementation Guide and to defining the rights, obligations, and responsibilities of Carequality Implementers and Carequality Connections (CCs). Implementers and CCs play a declared role or roles, and Implementers must indicate to Carequality, during the application process for each Use Case, which role or roles the Implementer will fill, and which role or roles each of its CCs fill.

Query Initiators fall into one of the following categories:

a. Principal: an Implementer or Connection that is acting as a (i) Covered Entity, (ii) Governmental Entity, (iii) a health care provider that meets the definition of such term in either 45 CFR § 171.102 or in the HIPAA Rules at 45 CFR § 160.103 but is not a Covered Entity, (iv) a Public Health Authority as defined in 45 CFR § 164.501, (v) an entity asserting the Coverage Determination Permitted Purpose (as authorized by an Individual), or (vi) an entity asserting the Patient Request or Other Authorization-Based Disclosures Permitted Purposes (as authorized by an Individual) when engaging in transactions via Carequality.
b. Delegate: a First Tier Delegate or Downstream Delegate.
    I. First Tier Delegate: an Implementer or Connection that (i) is not acting as a Principal when playing the role of Initiator or Responder in a transaction via Carequality and (ii) has been authorized by a Principal to play the role of an Initiator and, unless indicated in the Initiator Only Attestation, Responder in transactions via Carequality for or on behalf of the Principal for specified Permitted Purposes.
    II. Downstream Delegate: a Connection that (i) is not acting as a Principal when playing the role of an Initiator or Responder in a transaction via Carequality and (ii) has been authorized by a First Tier Delegate to play the role of an Initiator and, unless indicated in the Initiator Only Attestation, Responder in transactions via Carequality for or on behalf of a Principal for specified Permitted Purposes.

By default, any requirement specified within this document applies to all Implementers and CCs regardless of role or Use Case. Requirements that only apply to Implementers or CCs with a specific role(s) will be clearly indicated within the text.

An Implementer may fill different roles than its CCs, or may not actually fill any role at all. For example, an Implementer may provide network support, services, and oversight but play no direct role in the transactions specified for that Use Case.

For more on the exact nature of roles for each Use Case, please refer to the relevant Implementation Guide.

# 3.0 Customizable Principles of Trust

## 3.1. Permitted Purposes

Carequality Implementers and CCs represent a diverse set of stakeholders that wish to exchange health information for a variety of reasons. In order to establish trust, it is important to identify a shared set of acceptable reasons to initiate a request for information ("Permitted Purposes"). The Permitted Purposes allowed in any Use Case are:

- Treatment
- Payment
- Health Care Operations
- Public Health Activities
- Patient Request
- Coverage Determination
- Care Coordination
- Other Authorization-Based Disclosures

The first four terms are used as defined in the Health Insurance Portability and Accountability Act ("HIPAA") and its implementing regulations, 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E, *Standards for Privacy of Individually Identifiable Health Information*, and 45 C.F.R. Part 164, Subpart C, *Security Standards for the Protection of Electronic Protected Health Information.* Public Health Activities are those permitted pursuant to 45 C.F.R. Part 164.512(b).

An Implementer or CC may claim the Patient Request Permitted Purpose for queries that are directly initiated by the patient or the patient's personal representative as defined by 45 CFR 164.502(g), via a personal health record or other consumer-facing service. Note that any requests initiated by individuals other than the patient or personal representative may not use the Patient Request Permitted Purpose, even if the patient has indicated that he or she wishes for the request to occur. For queries initiated directly by the patient's personal representative, the Query Initiator is responsible for ensuring that the individual initiating the query is, in fact, authorized and appropriate to act as the personal representative as defined by HIPAA.

Implementers and CCs that initiate queries for the Permitted Purpose of Patient Request ("Patient Requesters") MUST provide their users with a clear description of how the user's data is used by the Patient Requester. This description must be an accurate representation of any data use permitted by the terms and conditions to which the user agrees, in order to use the Patient Requester's personal health record or other consumer-facing application. While not specifically requiring compliance with the current version of the CARIN Alliance Code of Conduct (the "Code of Conduct"), compliance with the Code of Conduct would fulfill this requirement. Implementers and CCs who wish to attest to compliance with the CARIN Code of Conduct may visit MyHealthApplication.com and apply to be published.

An Implementer or CC who is not a Covered Entity as defined by HIPAA may claim the Coverage Determination Permitted Purpose if the request is pursuant to an authorization as defined by

HIPAA, and the request is for the purpose of making a determination of eligibility for, or ongoing administration of, disability benefits, life insurance, or other insurance or similar benefits. Note that a health plan or other Covered Entity must claim the Payment Permitted Purpose when making requests for similar purposes. Also note that the primary intent of the Coverage Permitted Purpose is to inform Query Responders that the particular request is being made by an organization that is not a Covered Entity. Providing this level of detail allows Responders to make fully informed access policy decisions.

An Implementer or CC that initiates queries for the Permitted Purpose of Care Coordination, a subcategory of Health Care Operations as defined in 45 C.F.R. Part 164, Subpart E, may only do so if their query is a request for data initiated by a non-provider Covered Entity or BA to determine how to deliver care for a particular patient, group, or community by performing one or more actions in order to organize the provision and case management of an individual's healthcare, including: Monitoring a patient's goals, needs, and preferences; acting as the communication link between two or more parties (e.g. providers or case management companies) concerned with a patient's health and wellness; organizing and facilitating care activities and promoting self-management by advocating for, empowering, and educating a patient; and ensuring safe, appropriate, non-duplicative, and effective integrated care.

An Implementer or CC may claim the Other Authorization-Based Disclosures Permitted Purpose if the request is pursuant to an authorization as defined by HIPAA, and the request does not qualify for the Coverage Determination Permitted Purpose as defined above.

Not every Implementer will support all of the Permitted Purposes across every Use Case. Therefore, each Implementer shall identify to Carequality the Permitted Purposes that it and each of its CCs support per Use Case.

When an Implementer or CC initiates a query for information, it shall clearly identify the specific Permitted Purpose for the query as detailed in each respective Use Case Implementation Guide. By asserting a Permitted Purpose, an Implementer or CC certifies that the context of its request meets the requirements for the stated Permitted Purpose as defined above.

Note that the Permitted Purposes allowed for Carequality are a subset of those defined in the NHIN Authorization Framework, with the caveat that Other Authorization-Based Disclosures provides some additional flexibility. See the table below for additional information on the Other Authorization-Based Disclosures Permitted Purpose. The specific NHIN PurposeOfUse values that may be used to represent the Carequality Permitted Purposes are as follows:

| **Carequality Permitted Purpose** | **NHIN PurposeOfUse code** |
|---|---|
| Treatment | TREATMENT |
| Payment | PAYMENT |
| Health Care Operations | OPERATIONS |

| | |
|---|---|
| Public Health Activities | PUBLICHEALTH |
| Patient Request | REQUEST |
| Coverage Determination | COVERAGE |
| Care Coordination | CARECOORDINATION* |
| Other Authorization-Based Disclosures | The Implementer or CC may use any NHIN PurposeOfUse code that is NOT otherwise listed in this table and is not prohibited in the following paragraph, and that the Implementer or CC in good faith believes is the best available representation of the transaction's actual purpose. It is acknowledged that the available PurposeOfUse codes may not include a clearly obvious value for every transaction, and Carequality anticipates future work to more clearly define specific values. NHIN PurposeOfUse codes are defined by the NHIN Authorization Framework 3.0 specification, section 3.2.2.6.<br><br>Notwithstanding the previous paragraph, **the following PurposeOfUse codes MUST NOT be used for Carequality:** PRESENT, EMERGENCY, DISASTER. |

* Note that "CARECOORDINATION" is not an NHIN PurposeOfUse Code, but one that Carequality has designed to accommodate Care Coordination exchange.

Note that the PurposeOfUse codes defined by the NHIN Authorization Framework encompass two separate concepts—the immediate use to which the information released will be put, and other attributes of the request that may impact the responder's access policies. Carequality divides these two concepts into the Permitted Purpose, and Access Policy Assertions (the latter being fully described below in Section 4.4). For example, Carequality has defined a Policy Assertion to indicate when a request is being made in an emergency situation. The information released in such a case is most likely going to be used for Treatment, so in Carequality's defined structure, the PurposeOfUse is Treatment, with a Policy Assertion of Emergency, potentially among others that may also apply.

## 3.2. Full Participation

It is important that all Implementers, CCs, and their End Users understand that others are committed to participating in Carequality Use Cases so that all those who participate can realize value for their investment of time and resources.

An Implementer or CC that plays the role of Query Responder for any Use Case, as defined in the relevant Implementation Guide, is strongly encouraged to provide information in response to queries for Treatment and Patient Request, unless doing so would violate Applicable Law or the

Implementer's or CC's local access policies. An Implementer or CC may provide information in response to queries for other Permitted Purposes, but is not required to do so.

#### 3.2.1. Treatment

An Implementer or CC wishing to assert the Treatment Permitted Purpose must provide one of the following pieces of evidence:

- Organization-level NPI (Type 2), or Provider-level NPI (Type 1) in cases where an Organization-level NPI is not needed and has not been acquired
- State-level certification/accreditation/licensure
- CLIA certification (for labs)

An organization that cannot provide evidence in one of the forms above may propose an alternative piece of evidence that could be applied generally to it, and similar organizations. This alternative may be considered by the Steering Committee as a possible addition to the list of accepted evidence above. An Implementer or CC is permitted to serve ONLY in the role of Query Initiator for the Permitted Purpose of Treatment if that Implementer or CC has received authorization from Carequality and:

(i) is a provider organization with no clinical information that could reasonably be made available for response as defined in Section 3.2.1.1 below;
(ii) is an EMS provider with alternative provision of data, as defined in Section 3.2.1.2 below;
(iii) initiates request On Behalf Of a Query Responder, as defined in 3.2.1.3 below;
(iv) is an Initiator Only Delegate, as defined in 3.2.1.4 below; or
(v) is otherwise prohibited from serving in the Query Responder role by Applicable Law.

An Implementer or CC, other than those defined below in the subsections of this Section 3.2.1, who wishes to be a Query Initiator for Treatment purposes in any Use Case MUST also play the role of Query Responder for the Treatment purpose and SHOULD play the role of Query Responder for Patient Request (as per section 3.6) and Care Coordination purposes in that Use Case.

An Implementer who is, or who provides access to, directly or via its CCs, one or more organizations that are subject to the exceptions listed in the previous paragraph, MUST list each such organization—as defined in this specific case to be the smallest separate business entity that, as a whole, meets the exception requirements—in the Carequality Directory as a distinct, separate entry. For clarity, note that an individual in solo practice could be an "organization" for purposes of this requirement. These entries must label the organization, in the Organization.extension:InitiatorOnly field, as one of the following values, as appropriate based on that organization's exception:

- Provider Organization (Initiator Only)
- EMS Provider (Initiator Only)
- On Behalf Of (Initiator Only)
- Delegate (Initiator Only)
- Other Authorized (Initiator Only)

Organizations that do not qualify for the exceptions listed in the previous paragraph MUST NOT be assigned these Organization.extension:InitiatorOnly values, so that the Carequality community can immediately discern which organizations are claiming an exception

#### 3.2.1.1. Provider Organizations Without Electronic Clinical Information

An Implementer or CC that is a healthcare provider organization is considered to have no available clinical information for response when clinicians within that Implementer or CC primarily maintain patient data on paper or otherwise outside of an EHR system, and the organization's staff are only able to initiate queries through a web portal or other mechanism provided by a third party. One possible example of this is a "stand alone" (i.e., not tied to an Implementer's EHR) Specialty Pharmacy. For additional clarity, an organization that maintains patient clinical data and supports clinician workflows with an electronic system does NOT qualify as having no clinical information for response, if the inability to respond is due to such electronic system's lack of support for the specifications outlined in the applicable Implementation Guide.

#### 3.2.1.2. Emergency Medical Services (EMS) Providers with Alternative Data Sharing Methods

An Implementer or CC is considered to be an EMS Provider if its primary healthcare activity is patient transport with paramedic support. For clarity, taxi and other transport services lacking skilled support are not EMS Providers. Additionally, organizations providing patient transport in addition to other healthcare services, such that patient transport is not the organization's primary healthcare activity, are not EMS Providers. Further, such EMS Provider is considered to have an alternative data sharing method if the organization to which the EMS Provider is transporting the patient can reasonably expect to receive a summary of any care provided in the course of transport in a format such that the summary can be included in the receiving organization's electronic record for the patient. Such formats include, but are not limited to, Direct message and fax. Failure to provide a summary in isolated cases does not disqualify an EMS Provider from having an alternative data sharing method, as long as the organization to which the patient is being transported can reasonably expect such a summary.

#### 3.2.1.3. On Behalf Of

An Implementer or CC is considered an On Behalf Of (OBO) entity when the healthcare providers utilizing the OBO entity primarily maintain patient clinical information in another system (e.g., an EHR used as system of record), the OBO entity is able to initiate queries, but the OBO entity has no information to share as a Responder due to no new clinical information being entered into or created by the OBO system. For clarity, if a Query Initiator produces or derives new clinical data then that entity is not eligible for this exception.

An OBO entity may only initiate queries on behalf of an organization that is currently published as a Responder in the Carequality Directory. The OBO organization in the Directory must point to the OID of the organization that it queries on behalf of as defined in the Carequality Directory IG. Beginning on May 12, 2025, before listing any new OBO entry in the Carequality Directory, the Implementer of the OBO entry and the Implementer of the Principal on whose behalf the OBO entry is acting must receive a Delegation Notice from the Principal. By August 12, 2025, any existing OBO

entry that is a Delegate in the Carequality Directory prior to May 12, 2025 must be identified in a Delegation Notice from the respective Principal to continue exchanging on behalf of such Principal through Carequality.

An Implementer that publishes OBO entities to the Carequality Directory prior to moving to the R4 version MUST use the following naming convention:

[Organization Name as intended to display in Directory] #OBO# [Directory OID of Responding organization]. The string "#OBO#" MUST NOT be used in the name of any non-OBO entity.

An OBO entity may only query for a patient that corresponds to a patient record that exists in the responding system on whose behalf the OBO entity is initiating queries. If an OBO entry's referenced organization objects in any way to that relationship, the OBO entry MUST remove the reference to that CC or suspend their use of Carequality until the responding organization has confirmed the relationship with Carequality.

OBO entities MUST comply with the Information Handling Transparency requirement in Section 14 of the CCA, as if the OBO entity were an Implementer.

This Section 3.2.1.3 will remain in effect until September 22, 2025, at which time it will no longer be in effect.

#### 3.2.1.4. Initiator Only Delegate

Delegates seeking to use the Initiator Only Delegate exemption MUST provide an Initiator Only Attestation Form (see Section 3.7.3). This attestation is provided by a Principal to its Implementer attesting the data obtained or created by the Principal's Delegate that becomes part of a Designated Record Set of a Principal is shared through Carequality by the Principal's system that is identified in such attestation. For purposes of the Initiator Only Attestation, Designated Record Set has the meaning assigned to that term in 45 CFR §164.501 but applies to a Principal regardless of whether the Principal is a Covered Entity.

## 3.3. Permitted Users

If supported for a particular Use Case, additional details regarding Permitted Users will be denoted in the relevant Implementation Guide. Otherwise, it is up to the Implementers and CCs to design and implement their respective organizational workflows for accomplishing a Permitted Purpose.

## 3.4. Data Sufficiency and Integrity

It is clear to all stakeholders that the health information stored in EHRs would be more easily transacted over data sharing networks if the information were better structured into universally accepted formats. The industry has not yet universally adopted and implemented consistent content standards. The clear goal of Carequality is to make progress toward greater consistency and quality in data content over time.

To this end, Carequality enforces requirements related to data content. Carequality will utilize one or more Carequality approved testing programs to validate that specific categories of organizations,

defined by the testing program, are able to produce content that conforms to Carequality's requirements.

Responding organizations should return patient summary and/or encounter summaries, as appropriate, as defined in Carequality's content guide, Concise Consolidated CDA: Deploying Encounter Summary and Patient Summary Documents with Clinical Notes, as available and in accordance with Applicable Law.

The Use Case Content Testing Program will define which categories of Implementer and/or their CCs are required to submit to content testing. Implementers or CCs that fall into one or more of these categories are required to test within the timelines defined by the program. Failure to submit to testing or to comply with test result recommendations may result in an organization's removal from live exchange activities. Generally, and independent of the specific data format used, Query Responders MUST ensure that data returned in response to queries provide an accurate representation of the information contained in the responding system at the time of data generation.

It is recognized that different types of organizations capture and maintain varying amounts of clinical data based on their role in patient care, including specialty and other functions performed. Responders satisfy their obligation under Full Participation for Treatment by contributing fully and completely with respect to data or resources available within their system, and when available, by properly utilizing directory flags, defined in the current Directory Implementation Guide, to indicate what to expect in response. The Responder shall respond in accordance with Carequality content requirements or, if no such content requirements are specified, in another industry-standard format, as available. While not required, Query Initiators for the Permitted Purpose of Care Coordination SHOULD respond to queries from others and make data available in the form of a CDA, C-CDA, PDF, or FHIR resource via the appropriate Carequality Use Case(s) in alignment with any reciprocity expectations of the Responding organizations that they request information from.

For example, a lab system is allowed to return a C-CDA document containing only known details of orders and results, without including other clinical information required within the C-CDA template, but not collected in their system. The response is still required to be a fully compliant C-CDA document.

When a Responder has limited technical capacity and can only reply with an unstructured CDA or a PDF, it is preferred that the response come in the form of a PDF or other plain document (i.e., jpeg, etc.) with the appropriate format code and MIME type.

## 3.5. Secondary Use and Disclosure

Implementers and their CCs may use patient data beyond the purpose for which it was originally obtained, only if the secondary use complies with Applicable Law. Carequality will review any complaints as part of the Carequality Dispute Resolution Process. Carequality reserves the right to take punitive actions including, but not limited to, suspension or denial of exchange access to any organization(s) that are found to violate this Policy.

## 3.6. Patient Request – Identity Verification and Demographics

As specified in the Carequality Connected Agreement (CCA) for Implementers and the Carequality Connection Terms for CCs, all Implementers and CCs, including those playing the Initiator role for Patient Request queries in any Use Case, must comply with the provisions of the HIPAA Regulations that are applicable to Business Associates as a minimum contractual standard of conduct even if the Implementer or CC is not a Covered Entity, a Business Associate, or a Governmental Entity.

Implementers or CCs initiating queries for the Patient Request Permitted Purpose are required to partner with a Credential Service Provider (CSP) that has been vetted and approved by a certifying body selected by Carequality. Currently, the Kantara Initiative is the only approved certifying body. Other approved certifying bodies will be posted to the Carequality website. Patient Request end users must be verified to at least IAL2 and authenticated to at least AAL2 as described in NIST SP 800-63. IAL2 verification MUST be completed by the CSP; AAL2 authentication may, but is not required to be, conducted by the CSP.

Patient portals (typically connected to an EHR/EMR) that allow patients to directly exchange information in any Use Case must verify patients through a CSP in the same way as other Patient Request Initiators. These organizations may incorporate this step as part of provisioning the patient's portal access, or work with a certifying body to become listed as a CSP in their own right. Initiators interested in providing proxy access to patient records, for example to a parent or other authorized representative, MUST utilize Carequality's FHIR Use Case. Please see Carequality's FHIR Use Case for further details on this approach.

Note: A CSP is only required when asserting a patient's identity externally, leveraging demographics or patient ID-based transactions, outside of a portal credential flow. For clarity, a CSP is not required when:

1) The patient is accessing data already contained in the Consumer App's system, or

2) When using portal credentials issued by the data holder to authenticate the patient and retrieve their records.

If the patient or app wishes to allow the patient to query for data with demographics and/or patient IDs without the use of portal credentials, then a CSP shall be used.

### 3.6.1. Demographic Matching within Patient Request

Until a standard to separate verified from non-verified demographics exists, Initiators must only use verified demographics for Patient Request queries. Implementers and CCs playing the role of Initiator for the Patient Request permitted purpose, may only assert demographics that have been verified by their CSP. After a successful identity validation event, the CSP must supply the Initiator with a technical token (IAL2 Claims Token as defined in the Technical Trust Policy) containing the verified demographics as described in the Technical Trust Policy. These demographics, once verified, will be immutable. Any change (such as a change of address) will require verification by their CSP. Any historical demographic that has been verified by the CSP at any point in the past can be used, even if that demographic has been changed or is otherwise outdated, so long as a non-

expired matching token is asserted along with it. It is recommended, but not required, that Consumer Applications/PHRs/other Patient Request Initiators prompt their patients to periodically verify that their demographics are up to date.

Implementers and CCs playing the Responder role to a Patient Request Query may only match based on the approved set of demographics for Patient Request queries. Responders MAY use any of the items in the Demographics Superset list for matching, however, they MUST NOT require any individual item not included in the "Must" section of that list. Responders MAY use fewer than the full list of demographics, but they may not require additional demographic types to achieve an acceptable match as defined by the Responder's patient matching algorithm. If a Responder's patient matching algorithm achieves an acceptable and unique match on these demographics, they should respond. The only exception to this is in the instance of an unambiguous conflict (ex. Twins). Responders may, but are not required, reject queries in cases where the demographics within the query body DO NOT match those contained within the token.

**Demographic Superset**

| | |
|---|---|
| Queries for Patient Request MUST include these verified demographics | First Name, Last Name, Date of Birth, Address, City, State, ZIP |
| Queries for Patient Request MAY include these verified demographics | Middle Name, Middle Initial, Suffix, Email Address, Mobile Phone Number, SSN, SSN last 4 digits, ZIP+4, Sex, and Other Verifiable Identifiers (ex. Passport Number, Driver's License, or State ID) |

Implementers and CCs that play the Initiator role for Patient Request must have a method for their end users to report data in their record that they suspect belongs to another individual. If an unauthorized disclosure is found by the Initiator, they must notify the Implementer and/or CC that was the source of the disclosed data via a secure channel in a timely manner. This notification must minimally include:

- A brief description of what happened, including the date of the disclosure and the date of the discovery of the disclosure, if known
- Transaction details that can be utilized for traceability including type of data involved, the transaction ID, receiver, date, and time

## 3.7. Delegation of Authority

An Implementer or CC that meets the definition of a Principal may authorize a First Tier Delegate to be an Initiator or Responder on behalf of the Principal. An Implementer or CC that meets the definition of a First Tier Delegate may authorize a Downstream Delegate to be an Initiator or Responder on behalf of the Principal if the First Tier Delegate is authorized to do so in the Principal's applicable Delegation Notice. To be able to authorize a Delegate to send Delegated Requests on behalf of the Principal, the Principal MUST, independent of the Delegate, play the role

of Query Initiator for the Permitted Purpose for which the Delegate will act on behalf of the Principal.

#### 3.7.1. Delegation Notices and Revocations

The association between a Principal and a Delegate is confirmed through a Delegation Notice(s), which is a notice provided by a Principal to its Implementer that the Principal wants to authorize a Delegate to initiate Delegated Requests on behalf of the Principal. By submitting a Delegation Notice, the Connection submitting the Delegation Notice is attesting that it is authorizing the Delegate to conduct transactions via Carequality for or on behalf of a Principal.

A Principal is responsible for providing the Delegation Notice to its Implementer when the Principal wants to authorize a First Tier Delegate to initiate Delegated Requests in connection with the services provided by the First Tier Delegate to the Principal. A First Tier Delegate is responsible for providing the Delegation Notice to its Implementer when the First Tier Delegate wants to authorize a Downstream Delegate to initiate Delegated Requests in connection with the services provided by the Downstream Delegate to the First Tier Delegate making the notification to its Implementer. A First Tier Delegate may only authorize a Downstream Delegate for a specific Principal if that Principal has authorized the use of a Downstream Delegate in the applicable Delegation Notice submitted by the Principal for the respective First Tier Delegate.

A Delegation Notice must be signed by an individual(s) who has the requisite signing authority for the Connection submitting the Delegation Notice. An Implementer may not require that a Delegation Notice be signed by more than two authorized individual(s) from the applicable Connection.

Upon receipt of a Delegation Notice, the Implementer MUST inspect the Delegation Notice for completeness and validity and notify the Connection of its determination within five (5) business days.

a. The Implementer MUST update the Carequality Directory within one (1) business day of determining the Delegation Notice to be complete and valid. Beginning on the applicable date set forth in Section 3.7.5, the Carequality Directory must be updated by the Implementer by listing the First Tier Delegate or Downstream Delegate within the Directory entry of the Connection submitting the Delegation Notice. The Directory Entry of the Connection submitting the Delegation Notice must use the "Delegation of Authority (DOA)" extension with reference to the Organization resource(s) for the Delegate named in the Delegation Notice.

b. If the Implementer determines that the Delegation Notice is incomplete and additional information is required to validate the legitimacy of the Delegation Notice, the Implementer MUST request such information from the Connection that submitted the Delegation Notice by the end of fifth (5th) business day after receipt.

c. If the Implementer determines that the Delegation Notice lacks the signature(s) of an individual(s) with the requisite signing authority for the Connection, the Implementer MUST notify the Connection that submitted the Delegation Notice by the end of the fifth ($5^{th}$) business day after receipt and provide to the Connection the name(s) of the individual(s) who the Implementer

believes has the requisite signing authority for the Connection. The Implementer MUST also simultaneously provide such information to the Implementer of the Delegate named in the Delegation Notice.

Implementers must cooperate with other Implementers, the Delegate, and the Principal during the validation process and keep each other apprised of any discrepancies and path to resolution.

In instances where a Connection wants to remove a Delegate's authorization to initiate Delegated Requests on behalf of the Connection, the Connection will provide notice to its Implementer in the form of a Delegation Revocation. Upon receipt of a Delegation Revocation from an authorized individual, the Implementer must update the Carequality Directory within one (1) business day to remove the Delegate as a Directory Entry of the Connection submitting the Delegation Revocation.

#### 3.7.2. Delegated Requests

A Query initiated by a Delegate working, directly or indirectly, for a Principal ("Delegated Requests") MUST follow all requirements that apply to the Principal, as set forth in the Carequality Connection Terms and Carequality Framework Policies. This means that if the Delegate plays the role of an Initiator, it must also play the role of a Responder except to the extent that the Principal has provided an Initiator Only Attestation for the Delegate. Delegates MUST also comply with the Information Handling Transparency requirement in Section 14 of the CCA, as if the Delegate were an Implementer.

The Principal's listing in the Carequality Directory MUST point to the OID of the Delegate, or a First Tier Delegate's listing must point to the OID of a Downstream Delegate, using the Delegation of Authority (DOA) extension, as defined in the Carequality Directory Implementation Guide.

All Delegated Requests MUST list the Principal for whom the Delegate is initiating the Delegated Request. The Delegate's Implementer MUST verify that the Principal referenced in the transaction matches a Principal listed in the Carequality Directory and that the Principal has identified the Delegate as such in the Carequality Directory (or that the Principal's First Tier Delegate has identified a Downstream Delegate). A transaction from a Delegate that does not appropriately reference a Principal MUST NOT be accepted.

To list the Principal for whom the Delegate is initiating the Delegated Request, the Delegate and its Implementer will append the following within the SAML for each Delegated Request:

> This <Attribute> element MUST have the Name set to "QueryAuthGrantor". The value MUST be the FHIR Organization Resource ID from the Carequality Directory listing assigned to the Principal for whom the Delegate is initiating the Delegated Request.
>
> <saml:Attribute Name="QueryAuthGrantor">
>
> <saml:AttributeValue>Organization/2.16.840.1.113883.3.7204.1</saml:Attribute Value>
>
> </saml:Attribute>

### 3.7.3. Delegation Notice and Initiator Only Attestation Form- Principal to First Tier Delegate

Principal's Name:

Principal's Implementer:

First Tier Delegate Entity Name:

First Tier Delegate Entity's Implementer:

First Tier Delegate's OID:

Carequality permits a Principal to delegate to a third party (the "Delegate") the right to query for records on behalf of the Principal through Carequality. The Delegate must also respond to queries on behalf of the Principal unless the Principal confirms that the Delegate is an "Initiator Only." This Form must be completed by the Principal and returned by the Principal to its Implementer to document the Principal's identification of a Delegate. For more information about Principals, Delegates and Delegation of Authority in Carequality, please talk with your Implementer or see www.carequality.org.

1. **Authorized Permitted Purposes**. Principal authorizes the Delegate to play the role of an Initiator and, unless indicated in the Initiator Only Attestation, Responder in transactions via Carequality for or on behalf of the Principal for the following Permitted Purposes (check all that apply):
    - ☐ Treatment
    - ☐ Payment
    - ☐ Health Care Operations
    - ☐ Public Health Activities
    - ☐ Patient Request
    - ☐ Coverage Determination
    - ☐ Care Coordination
    - ☐ Other Authorization-Based Disclosures

2. **Principal's Participation in Carequality for Treatment**. If the Principal is authorizing the Delegate for a Permitted Purpose, then the Principal MUST also be an Initiator in transactions via Carequality for such Permitted Purpose. By checking the box below, the Principal is attesting that it is an Initiator in transactions via Carequality for the Permitted Purpose(s) identified above.
    - ☐ Principal is an Initiator in transactions via Carequality for the Permitted Purpose(s) identified above.

3. **Initiator Only**. By checking the box blow for the Initiator Only Attestation, the Principal is attesting that the Delegate does not create or derive any new clinical information nor is the Principal entering or maintaining new clinical information in the Delegate's system. Principal confirms that data obtained by the Delegate that becomes part of Principal's Designated Record Set is shared with and maintained by the Principle in the system that the

Principal utilizes to respond to queries for the Permitted Purposes indicated above through Carequality. Principal MUST notify its Implementer immediately in the event this Attestation is no longer accurate or complete.

For purposes of this Initiator Only Attestation, Designated Record Set has the meaning assigned to that term in 45 CFR §164.501 but applies to a Principal regardless of whether the Principal is a Covered Entity.

☐ Initiator Only Attestation

4. **Downstream Delegate**. By checking the box below for Downstream Delegates, the Principal is authorizing the Delegate named in this Form to appoint its own Delegate (a "Downstream Delegate") to play the role of an Initiator and, unless indicated in the Initiator Only Attestation, Responder in transactions via Carequality for or on behalf of the Principal for the Permitted Purposes identified above.

   ☐ Downstream Delegate is authorized.

Signed by the Principal's Authorized Individual:

Signature:

Name:

Title:

Date:

(Optional) Signed by the Principal's Authorized Individual:

Signature:

Name:

Title:

Date:

### 3.7.4. Delegation Notice Form – First Tier Delegate to Downstream Delegate

Principal's Name:

Principal's Implementer:

First Tier Delegate Name:

First Tier Delegate Implementer:

Downstream Delegate Entity Name:

Downstream Delegate Entity's Implementer:

Downstream Delegate's OID:

1. **Authorized Permitted Purposes**. First Tier Delegate authorizes the Downstream Delegate to play the role of an Initiator and Responder in transactions via Carequality for or on behalf of the Principal for the following Permitted Purposes (check all that apply):
    - ☐ Treatment
    - ☐ Payment
    - ☐ Health Care Operations
    - ☐ Public Health Activities
    - ☐ Patient Request
    - ☐ Coverage Determination
    - ☐ Care Coordination
    - ☐ Other Authorization-Based Disclosures

Signed by the First Tier Delegate Authorized Individual:

Signature:

Name:

Title:

Date:

(Optional) Signed by the First Tier Delegate Authorized Individual:

Signature:

Name:

Title:

Date:

Example: Southeast Health System has two EHR systems, one of which is connected to Carequality through Implementer B as both an Initiator and Responder for Treatment ("EHR 1") and one of which is not connected to Carequality ("EHR 2"). Southeast Health System uses a Delegate that provides a care management system to create care plan for specific diabetic patients (the "Delegate Care Manager"). All data obtained by the Delegate Care Manager and the resulting care plans are maintained in the Delegate Care Manager's system. In addition, the data and resulting care plans are sent back to the respective EHRs in which the Individual's data resides (e.g., either EHR 1 or EHR 2). Because EHR 1 is connected to Carequality as an Initiator and Responder, the Principal can provide an Initiator Only Attestation for the Delegate Care Manager and the Delegate Care Manager can be an Initiator Only with respect to Individuals whose records reside in EHR 1. Because EHR 2 is not connected to Carequality and is not a Responder, an Initiator Only Attestation is not available for the Delegate Care Manager with respect to Individuals whose records reside solely in EHR 2. As a result, to play the role of an Initiator through Carequality for individuals whose records reside in EHR 2, the Delegate Care Manager must be an Initiator and Responder.

Example: Dr. Smith at Peaceful Valley Hospital maintains all clinical records in the hospital's EHR system, which is a Carequality Connection. Dr. Smith also leverages a data visualization app that takes in outside information to assist with clinical workflows, but all new clinical information is entered and maintained in the hospital EHR system. The data visualization app, with no new information to share would be an Initiator Only, pointing to the Peaceful Valley Hospital OID as the Responder on whose behalf the app queries.

#### 3.7.5. Implementation Timeframes

Effective Date – May 12, 2025:

- No new OBO entries can be published unless the OBO's Implementer and the Principal's Implementer have received a Delegation Notice and the Principal's Implementer has confirmed to the OBO's Implementer that the Delegation Notice is complete. When publishing a new OBO entry, the OBO's Implementer must comply with Section 3.2.1.3 regarding Directory naming conventions or the Carequality Directory Implementation Guide, whichever is applicable based on the version of the Directory in use by the OBO's Implementer.
- No new Initiator Only Delegates can be published unless the Delegate's Implementer and the Principal's Implementer have received a Delegation Notice and the Principal's Implementer has confirmed to the Delegate's Implementer that the Delegation Notice is complete. When publishing a new Initiator Only Delegate, the Delegate's Implementer must comply with Section 3.2.1.3 regarding Directory naming conventions or the Carequality Directory Implementation Guide for OBO, whichever is applicable based on the version of the Directory in use by the Delegate's Implementer.
- No new Delegate can be published unless the Delegate's Implementer and the Principal's Implementer have received a Delegation Notice and the Principal's Implementer has confirmed to the Delegate's Implementer that the Delegation Notice is complete. When publishing a new Delegate, the Delegate's Implementer must specify the Principal using the

Delegation of Authority (DOA) extension, as defined in the Carequality Directory Implementation Guide.
- All Implementers must comply with Section 3.7.1 related to the timelines for processing Delegation Notices.

July 14, 2025:

- Implementers SHOULD have an active representative environment(s) in the Staging Directory that can respond to both non-Delegated and Delegated Requests.
- Implementers with Delegates SHOULD have example Delegate(s) in the staging directory that can initiate Delegated Requests to help validate.
- Each Implementer MUST identify all of its Connections existing as of May 12, 2025 that are Delegates (including those play the role of Initiator and Responder) and provide a list of such Delegates to Carequality by July 14, 2025.

August 12, 2025:

- All OBOs and Delegates in the Directory MUST have a Delegation Notice that has been provided to the Delegate's Implementer and the Principal's Implementer and the Principal's Implementer has confirmed to the Delegate's Implementer that the Delegation Notice is complete. If an OBO or Delegate does not have a valid Delegation Notice for a Principal, it may not request records on behalf of such Principal.
- All Implementers with responding endpoints MUST have active representative environment(s) in the Staging Directory that can respond to both non-Delegated and Delegated Requests.
- Implementers with Delegates MUST have example Delegate(s) in the staging directory that can initiate Delegated Requests to validate connectivity.
- SAML partner testing begins for Implementers that intend to have Delegates.

September 15, 2025:

- Implementers must provide to Carequality evidence that it has successfully completed any testing related to Delegated Requests that is required by Carequality.
- Implementers of Principals begin adding Delegate pointers into the Carequality Directory and coordinate with Implementers of Delegates and OBOs for them to remove their pointers to the Principals from the Carequality Directory.
- Implementers must be able to successfully receive and respond to Delegated Requests.

September 22, 2025:

- All Delegation of Authority pointers in the Carequality Director must point from the Principal to the Delegate, all Delegated Requests MUST list the Principal for whom the Delegate is initiating the Delegated Request, the Delegate's Implementer MUST verify that the Principal referenced in the transaction matches a Principal listed in the Carequality Directory and that the Principal has identified the Delegate as such in the Carequality

Directory (or that the Principal's Delegate has identified a Downstream Delegate). A transaction from a Delegate that does not appropriately reference a Principal MUST NOT be accepted.

- All OBO entries MUST be removed from the Directory.
- Section 3.2.1.3 is sunset and no new OBOs are permitted.

Notwithstanding the foregoing, the Steering Committee may extend the implementation timeframes without amending this policy by providing notice to all Implementers.

# 4.0 Non-Discrimination

Interoperability is impaired if organizations are free to impose whatever terms they choose as a condition of exchanging information. All Carequality Implementers and CCs that choose to participate in a Use Case will do so without imposing unfair or unreasonable conditions that would limit exchange or interoperability with other Carequality Implementers and CCs that are similarly situated. A condition is unfair or unreasonable if it results in similarly situated Implementers, or their CCs, being treated differently. Whether two Implementers or CCs are similarly situated is determined primarily by the purpose for which the information is being exchanged, although other considerations may apply in specific circumstances as described below. In addition, notwithstanding any of the following general policies and/or examples, nothing in this section negates the obligation of all Carequality Implementers and CCs to comply with all Applicable Law for purposes of all exchange activities under the Carequality Framework, regardless of the Permitted Purpose and/or the type of organization acting in the role of initiator or responder. Such Applicable Law includes, but is not limited to, the information blocking regulations at 45 C.F.R. Part 171 with respect to Carequality Implementers and/or CCs that meet the definition of an "Actor" under 45 C.F.R. § 171.102.

## 4.1.Treatment

Carequality has the goal of enabling widespread exchange of health information on a nationwide scale, between many partners who do not have any direct relationship with one another outside of Carequality. Recognizing that the time and effort required to reach individual contractual agreements, including agreements whose purpose is to define fee payment terms, between all of these potential partners can be a barrier to widespread exchange, Implementers and CCs are prohibited from imposing any additional fees, terms or conditions on other Implementers or CCs with respect to queries or responses for the Permitted Purpose of Treatment. No additional agreements beyond the Carequality legal framework may be required. The type of organization initiating the query is not a factor (although organizations claiming the Treatment Permitted Purpose must actually be providing treatment or be making the request on behalf of a network member that is providing treatment).

> For example, suppose that Peaceful Valley Hospital has a record for John Smith. Peaceful Valley Hospital has been queried for this record by physician practices Adventist Medical and Children First. If Adventist Medical and Children First are both querying for Treatment, non-discrimination requires that these two practices should have equal access to Mr.

Smith's information. Mr. Smith may authorize release to a specific practice, but Peaceful Valley may not have an overall policy that treats the two practices differently.

## 4.2. Other Permitted Purposes

Implementers and CCs are permitted, but not required, to impose fees, terms and conditions on other Implementers or CCs with respect to queries or responses for any Permitted Purpose other than Treatment or Patient Request. Any fees, terms and conditions must comply with Section 4.3 of this Policy.

As mentioned in section 3.2, Implementers or CCs that play the role of Query Responder are not required to honor queries for non-Treatment Permitted Purposes. However, Implementers or CCs that are Query Responders may choose to honor queries for other Permitted Purposes.

The content provided in response to queries for non-Treatment Permitted Purposes may be the same content released in response to Treatment queries, though Implementers and CCs may also respond with an information set that is specific to a query's Permitted Purpose. Implementers and CCs may also choose to do so in order to comply with that Implementer's or CC's Applicant Business Rules or Organization Business Rules, as consistent with Applicable Law.

Additionally, Implementers responding to non-Treatment queries may apply patient matching logic that differs from those used in response to Treatment. Implementers and CCs in the Query Responder role MAY utilize separate patient matching logic for queries with different Permitted Purposes, for example, requirements that are more stringent and/or rely on exact matches for certain fields when responding to queries for Patient Request versus Treatment.

Query Responders MAY decline to honor queries for the Permitted Purposes of Payment, Health Care Operations, or Care Coordination for those patients who have received self-pay care, although Query Responders are encouraged to respond with those portions of the record that don't relate to the self-pay care.

If a Query Responder does choose to honor queries for a non-Treatment Permitted Purpose, it must honor queries for that Permitted Purpose from **all** Query Initiators, unless:

(i) to do so would violate Applicable Law;
(ii) it has chosen to honor queries only from particular government agencies, as further outlined in Section 4.3;
(iii) it has chosen to impose terms and conditions on Query Initiators, and has not reached agreement on such terms and conditions with a particular Query Initiator, as further described in Section 4.3; or
(iv) the Permitted Purpose is Other Authorization-Based Disclosures.

Note: Carequality anticipates further work to more fully define the Other Authorization-Based Disclosures Permitted Purpose. Until such additional definition is completed, Query Initiators may, in good faith, make queries using the same PurposeOfUse value that in fact stem from very different circumstances. Given this uncertainty, Query Responders are given considerable latitude to choose which queries to honor under this Permitted Purpose. Query Responders are strongly encouraged,

however, to honor queries for this Permitted Purpose equally from any organization, when the circumstances for the queries are generally similar.

### 4.3. Consistency in Additional Terms and Conditions

If an Implementer or CC chooses to impose additional terms and conditions on other Implementers and CCs with respect to performing or responding to queries for Permitted Purposes other than Treatment, such terms and conditions cannot vary based on the type of organization that the other Implementer or CC is. For example, a Query Responder cannot impose one set of conditions on health care providers and another set of conditions on health care payers for queries based on the same Permitted Purpose. However, acknowledging that some Permitted Purposes are quite broad, a Query Responder's terms and conditions may limit its responses to queries for that Permitted Purpose to specific workflows or types of data use, which may in turn result in the Query Responder only exchanging, in practice, with specific types of organizations. For example, queries by health plans for case management, queries by home health services in support of intake processes, and queries by EMS services in support of post-event staff training follow-up, could all arguably fall under the Permitted Purpose of "Operations." As long as a Query Responder's terms and conditions focus on a particular workflow as elucidated by the examples above – although not limited to the examples above – and do not exclude a particular organization or organization type that engages in the relevant workflow, such terms and conditions are acceptable under these non-discrimination requirements.

In addition, it may be acceptable for a Query Responder to treat local, state, tribal, or federal government agencies differently from other Implementers and CCs. For example, a Query Responder may choose to respond to queries for the Permitted Purpose of Payment from CMS but not from commercial insurers, provided doing so does not result in use of the Carequality Framework in violation of Applicable Law. Also, a Query Responder may accept a fee for providing information in response to a query from the Social Security Administration without charging a fee to other Query Initiators.

Except as noted above with respect to government agencies, additional terms and conditions must be imposed consistently on all other Implementers and CCs that perform or respond to queries for the same Permitted Purpose.

An Implementer or CC may impose different fees on different Implementers and CCs, but the differences must be based on a consistently applied set of objective, economically relevant criteria such as organization size or transaction volume.

If an Implementer or CC offers particular terms to one party, it must make good faith efforts to reach similar terms with other parties who perform or respond to queries for the same Permitted Purpose, subject to the exception for government agencies noted above. If a party feels that good faith efforts to reach terms are not being made, it may file a Dispute under the Carequality Dispute Resolution Process.

## 4.4. Access and Patient Permission

This Section outlines requirements for Implementers and CCs who wish to communicate access policy requirements and their fulfillment within query and response transactions. Implementers and CCs have discretion under Carequality's local autonomy principle to define access policies that may restrict the release of information for specific patients to other Implementers and CCs, with the limitation that such access policies may only be based on clinical or legal sensitivity of the information, or on the required patient permission that may be needed for the information to be released. Throughout this and other sections of this Policy and applicable Implementation Guide(s), the phrase "Patient Permission form" refers to a form that provides the Query Responder with the requisite legal authority to exchange or release the patient's records. Depending on the circumstances, a Patient Permission form may be a consent form or an authorization, as the two terms are defined by HIPAA. Patient Permission forms must be signed by the patient in question or by the patient's personal representative (in accordance with 45 CFR 164.502(g)).

Unlike Section 4.3, this Access and Patient Permission Section refers to access policy decisions made for individual patients rather than agreements between organizations. The internal application of these access policies may be quite complex and highly variable among Query Responders, based on each Query Responder's definition of clinical and legal sensitivity of different elements of patient records. In general, however, there are four possible categories into which the access policies will fall for any given Permitted Purpose:

1) The Responder's access policies do not support access for the specific Permitted Purpose of the query, at all.
2) The Responder's access policies never allow the release of information for the asserted Permitted Purpose, without specific additional permission or other mitigating circumstances, such as a medical emergency.
3) The Responder's access policies prohibit the release of information for the asserted Permitted Purpose, without additional permission or other mitigating circumstances, based on attributes of the particular patient record being queried.
4) The Responder's access policies always allow the release of information to valid Carequality requesters for the asserted Permitted Purpose

If a Query Responder's policies for a permitted purpose fall into categories (1) or (4), there is no role for additional information from the Query Initiator, and the remainder of this Section is largely inapplicable for that Permitted Purpose. For Query Responders whose policies fall into categories (2) or (3), however, additional input from the Query Initiator could be essential in determining whether or not information may actually be released in response to any individual query. In order to provide such additional input in a consistent way, such that Query Responders may evaluate whether or not the disclosure aligns with local access policies, Carequality defines a set of specific policy assertions that are available to Query Initiators.

> For example, suppose that Peaceful Valley Hospital has a record for John Smith. Peaceful Valley Hospital has been queried for this record by physician practice Adventist Medical. As a matter of policy, Peaceful Valley Hospital will release patient files only if they receive

signed consent from the patient or the patient's personal representative (category 2). Upon receiving the query without an indication of a signed document, Peaceful Valley will request additional documentation in response or will not release John Smith's information to Adventist Medical.

### 4.4.1. Access Policy Assertions

In addition to asserting a Permitted Purpose, Implementers and CCs may also assert access policies. "Access Policy Assertions" are concepts defined by Carequality that represent standardized policy constructs accessible to all Implementers. These assertions provide detailed information to the Query Responder about the initiator's capabilities and permissions. If a Query Initiator meets the requirements for an Access Policy Assertion outlined in the table below, the Query Initiator must assert an Access Policy Assertion by including the unique Access Consent Policy Identifier listed for the Assertion within a Carequality message, as described in the relevant Use Case Implementation Guide.

Access Policy Assertions are intended to provide Implementers and CCs additional flexibility in their access policies. An Initiator might assert that their Permitted Purpose is "Treatment," but these assertions allow the Query Responder to make a distinction within those Treatment-based requests. An example is the difference between those requests that have corresponding signed release forms from those that do not. While restricting access to patient data based on Access Policy Assertions provides responders with additional flexibility, it is not intended (and is, in fact, not permitted) to be used to discriminate against any particular Query Initiator in accordance with the Non-Discrimination Section of this Policy.

Several of the Access Policy Assertions – those referring to a Patient Permission form being "available in band" – apply to situations in which the Query Initiator has collected a consent form and is able to provide a copy of that form to the Query Responder, upon request. In such cases, the details for its usage will be defined in the respective technical component(s) for the relevant Implementation Guide.

Query Initiators are strongly encouraged to support the inclusion of Access Policy Assertions in messages as soon as possible. Carequality will provide a field within the Carequality Directory entries for Query Initiators that will indicate whether or not that Query Initiator has the ability to support the Access Policy Assertion structure. All statements in this Policy referring to requirements for Query Initiators apply specifically and only to those Query Initiators who are listed in the Carequality Directory as supporting the inclusion of Access Policy Assertions in messages. Carequality is not, at this time, imposing a timeline within which all Query Initiators must support the inclusion of Access Policy Assertions in messages, but may do so in the future.

Query Initiators must assert all policy assertions for which the Query Initiator meets the requirements. Note: All policy assertions should be asserted individually, even when one policy implies compliance with another. For example, in the case of the Policy Assertions related to NIST Identity Assurance Levels (IALs), meeting the requirements for IAL3 implies that the requirements for IAL2 have also been met. Nonetheless, Query Initiators who can assert IAL3 should also assert

IAL2. Compliance with this practice will remove complexity and allow for forward compatibility in the Query Responder's rule evaluation.

| Policy Assertion | Access Consent Policy Identifier | Requirements for the Initiator |
|---|---|---|
| Verbal Consent | urn:oid:<br>2.16.840.1.113883.3.7204.1.1.1.1.1 | The patient who is the subject of the transaction must be physically (or virtually via telemedicine) present at the facility initiating the query and have provided clear verbal confirmation of their consent to have records released by the Query Responder to the Query Initiator. The verbal consent must have been provided directly to a staff member prior to initiating the query. |
| Collected Initiator's Signed Patient Permission Form<br><br>(Available in band) | urn:oid:<br>2.16.840.1.113883.3.7204.1.1.1.1.2 | The Query Initiator must have collected a Patient Permission form containing all of the elements required for it to be a valid consent or authorization, as appropriate, under HIPAA, signed by the patient or an authorized representative. The specific text of the form is at the Query Initiator's discretion, as long as it contains, at a minimum, the HIPAA required elements and complies with Applicable Law. An electronic copy of the Patient Permission form must be available for retrieval by the Query Responder as outlined in the relevant Use Case IG.<br><br>Note that technical issues preventing the retrieval of an individual document do not constitute a failure of the Query Initiator to meet the requirements for this Policy Assertion, as long as a pattern of consistent failures does not emerge such that the Query Initiator must reasonably expect that Query Responders may |

| | | |
|---|---|---|
| | | be unable to retrieve Patient Permission documents. |
| Collected Initiator's Signed Patient Permission Form<br><br>(**Unavailable** in band) | urn:oid:<br>2.16.840.1.113883.3.7204.1.1.1.1.3 | The Query Initiator must have collected a Patient Permission form containing all of the elements required for it to be a valid consent or authorization, as appropriate, under HIPAA, signed by the patient or an authorized representative. The specific text of the form is at the Query Initiator's discretion, as long as it contains, at a minimum, the HIPAA required elements. The Query Initiator does not support a mechanism for retrieving an electronic copy of the Patient Permission form within the scope of the transactions outlined in the relevant Use Case IG, and the Query Responder shall not assume that it will be able to retrieve the Patient Permission form prior to making its access policy decision on whether or not to release records in response to the Query Initiator's request. The Query Initiator shall, however, provide a copy of the form to the Query Responder in response to reasonable requests after the fact. |
| Collected Responder's Signed Patient Permission Form<br><br>(Available in band) | urn:oid:<br>2.16.840.1.113883.3.7204.1.1.1.1.5 | The Query Initiator must have collected a Patient Permission form signed by the patient or an authorized representative, with the text of the form being specified by the Query Responder to meet the Query Responder's access policy requirements. The Query Initiator must have documented evidence of the Query Responder's intent for the form to be used in this manner, either directly in the form of an email or other communication, or indirectly through the Query Responder's submission of the form or form text to a system or service that the Query Responder knows will distribute the form or |

| | | |
|---|---|---|
| | | form text for purposes of facilitating the use of this Policy Assertion. An electronic copy of the Patient Permission form must be available for retrieval by the Query Responder as outlined in the relevant Use Case IG. Note that technical issues preventing the retrieval of data do not constitute a failure of the Query Initiator to meet the requirements for this Policy Assertion, as long as a pattern of consistent failures does not emerge such that the Query Initiator must reasonably expect that Query Responders may be unable to retrieve Patient Permission forms. |
| Collected Responder's Signed Patient Permission Form<br><br>(**Unavailable** in band) | urn:oid:<br>2.16.840.1.113883.3.7204.1.1.1.1.6 | The Query Initiator must have collected a Patient Permission form signed by the patient or an authorized representative, with the text of the form being specified by the Query Responder to meet the Query Responder's access policy requirements. The Query Initiator must have documented evidence of the Query Responder's intent for the form to be used in this manner, either directly in the form of an email or other communication, or indirectly through the Query Responder's submission of the form or form text to a system or service that the Query Responder knows will distribute the form or form text for purposes of facilitating the use of this Policy Assertion. The Query Initiator does not support a mechanism for retrieving an electronic copy of the Patient Permission form within the scope of the transactions found in the technical sections of the relevant Use Case Implementation Guide, and the Query Responder shall not assume that it will be able to retrieve the Patient Permission form prior to making its access |

| | | |
|---|---|---|
| | | policy decision on whether or not to release records in response to the Query Initiator's request. The Query Initiator must, however, provide a copy of the Patient Permission form to the Query Responder in response to reasonable requests after the fact. |
| Collected Initiator's Signed Patient Permission Form<br><br>(**Available** for electronic request within 10 days) | urn:oid:<br>2.16.840.1.113883.3.7204.1.1.1.1.4 | The Query Initiator must have collected a Patient Permission form containing all of the elements required for it to be a valid authorization as defined by HIPAA, signed by the patient or an authorized representative. The specific text of the form is at the Query Initiator's discretion, as long as it contains, at a minimum, the HIPAA required elements. The Query Initiator supports a mechanism for retrieving an electronic copy of the Patient Permission form using the transactions found in the technical sections of the relevant Use Case IG, but is not able to provide a copy at the time of the request, and the Query Responder shall not assume that it will be able to retrieve the Patient Permission form prior to making its access policy decision on whether or not to release records in response to the request. The Query Initiator must, however, make a copy of the Patient Permission form available to the Query Responder in response to an appropriate query after no more than 10 business days. |
| Collected Responder's Signed Patient Permission Form<br><br>(**Available** for electronic request within 10 days) | urn:oid:<br>2.16.840.1.113883.3.7204.1.1.1.1.7 | The Query Initiator must have collected an unaltered Patient Permission form signed by the patient or an authorized representative, with the text of the form being specified by the Query Responder to meet the Query Responder's access policy requirements. The Query Initiator |

| | | |
|---|---|---|
| | | must have documented evidence of the Query Responder's intent for the form to be used in this manner, either directly in the form of an email or other communication, or indirectly through the Query Responder's submission of the form or form text to a system or service that the Query Responder knows will distribute the form or form text for purposes of facilitating the use of this Policy Assertion. The Query Initiator supports a mechanism for retrieving an electronic copy of the Patient Permission form using the transactions outlined in the technical sections of the relevant Use Case IG but is not able to provide a copy at the time of the request, and the Query Responder shall not assume that it will be able to retrieve the Patient Permission form prior to making its access policy decision on whether or not to release records in response to the request. The Query Initiator must, however, make a copy of the Patient Permission form available to the Query Responder in response to an appropriate query after no more than 10 business days. |
| Public Health Emergency | urn:oid:<br>2.16.840.1.113883.3.7204.1.1.1.1.8 | The Query Initiator must be making its request for information in the context of a state of emergency that has been declared by state or federal officials. The specific patient who is the subject of the query must reasonably be associated with the declared emergency. For example, an outbreak of measles reaches an extent that it is declared a Public Health Emergency by local authorities. From this point on, queries in the affected area should include the Public Health Emergency policy assertion for |

| | | |
|---|---|---|
| | | patients who are impacted by the measles outbreak. Most such queries will likely be for Treatment, but could also be for the Public Health Permitted Purpose. Other Permitted Purposes are less likely to be aligned with this policy assertion, but the use of this assertion is not forbidden for other purposes, as long as the Query Initiator can reasonably claim that the query is associated with the declared emergency. |
| Emergency | urn:oid: 2.16.840.1.113883.3.7204.1.1.1.1.9 | The Query Initiator must be making its request in the context of an imminent threat to the health and safety of a patient or others as defined in 45 CFR 164.512(j)(1)(i). The Query Initiator must comply with reasonable follow-up requests from the Query Responder in order to comply with the Query Responder's regulatory obligations, including, without limitation, collecting a signed form after the fact or providing information on the nature of the emergency. |
| Patient Verified NIST Identity Assurance Level 2 | urn:oid: 2.16.840.1.113883.3.7204.1.1.1.1.10 | The Query Initiator must be making a request on behalf of the patient that is directly initiated within the Query Initiator's system by the patient. The Query Initiator must have verified the patient's identity in a manner compliant with NIST Identity Assurance Level 2, as described in NIST publication SP 800-63A. The Query Initiator may rely on a third party registration authority's identity verification but takes full responsibility for the identity verification complying with the NIST Identity Assurance Level 2. |

| | | |
|---|---|---|
| Authorized Personal Representative Verified NIST Identity Assurance Level 2 | urn:oid: 2.16.840.1.113883.3.7204.1.1.1.1.11 | The Query Initiator must be making a request on behalf of the patient as requested by the patient's authorized personal representative as described in 45 C.F.R. § 164.502(g) of the HIPAA Regulations. The personal representative's request must be directly initiated within the Query Initiator's system. The Query Initiator must have verified the personal representative's identity in a manner compliant with NIST Identity Assurance Level 2, as described in NIST publication SP 800-63A. The Query Initiator may rely on a third party registration authority's identity verification but takes full responsibility for the identity verification complying with the NIST Identity Assurance Level 2. |
| Patient Verified NIST Identity Assurance Level 3 | urn:oid: 2.16.840.1.113883.3.7204.1.1.1.1.12 | The Query Initiator must be making a request on behalf of the patient that is directly initiated within the Query Initiator's system by the patient. The Query Initiator must have verified the patient's identity in a manner compliant with NIST Identity Assurance Level 3, as described in NIST publication SP 800-63A. The Query Initiator may rely on a third party registration authority's identity verification but takes full responsibility for the identity verification complying with the NIST Identity Assurance Level 3. |
| Authorized Personal Representative Verified NIST Identity Assurance Level 3 | urn:oid: 2.16.840.1.113883.3.7204.1.1.1.1.13 | The Query Initiator must be making a request on behalf of the patient as requested by the patient's personal representative as described in 45 C.F.R. § 164.502(g) of the HIPAA Regulations. The personal representative's request must be directly initiated within the Query Initiator's system. The Query |

| | | |
|---|---|---|
| | | Initiator must have verified the personal representative's identity in a manner compliant with NIST Identity Assurance Level 3, as described in NIST publication SP 800-63A. The Query Initiator may rely on a third party registration authority's identity verification but takes full responsibility for the identity verification complying with the NIST Identity Assurance Level 3 (IAL 3). Note: All policy assertions should be asserted individually, even when one policy implies compliance with another. In the case of the Policy Assertions related to NIST IALs, while asserting IAL 3 implies compliance with IAL 2, the Query Initiator must assert both IAL 2 AND IAL 3. |
| Information from Substance-Abuse Facilities Covered Under 42 CFR Part 2 Can Be Accepted | urn:oid: 2.16.840.1.113883.3.7204.1.1.1.1.14 | The Query Initiator must be able to comply with requirements for handling information from substance abuse treatment facilities covered under 42 CFR Part 2 and, specifically, must be able to prevent the unauthorized disclosure of any such information outside the entity specifically identified as the requesting entity by virtue of the Home Community Identifier used in the query transactions. The Query Initiator must also be able to parse and interpret information contained in the metadata identifying the data as containing substance abuse treatment information as described in the relevant Use Case IG. |

In the case of any of the Policy Assertions involving a signed Patient Permission form, the Query Initiator is responsible for the thorough and accurate documentation of signatures and for the preservation of the form. Query Initiators must not assert policies related to having a signed form unless that form will remain valid, from the standpoint of an expiration date and time, for at least 24 hours after the assertion is made. Note: having the form explicitly revoked by the patient within

24 hours does not constitute a failure to meet this requirement. If the Query Initiator is unsure of a Patient Permission form's expiration date, it should not assume that a signed Patient Permission form is valid and, therefore, should not assert any Policy Assertions based on that form.

> For example, suppose that Peaceful Valley Hospital has a signed Patient Permission form from John Smith's personal representative, Jane Doe. When initiating any query to Adventist Medical, Peaceful Valley Hospital is responsible for assuring that Jane Doe is, in fact, an authorized representative of Mr. Smith. Additionally, when Peaceful Valley Hospital asserts that it has a signed Patient Permission form, it must also maintain a record of the expiration date for that data. If Peaceful Valley cannot determine an expiration date at a system level, it should not make the assertion. Adventist Medical should not consider any Patient Permission form assertion from Peaceful Valley to take precedence over the patient's decision to opt out of releasing records to Peaceful Valley.

Queries that assert NIST IAL 2 or 3 from a third party such as a PHR or a wearable device should be regarded as queries made directly by the patient. Unlike Patient Permission form assertions, IAL assertions do not require the same expiration dates restrictions.

> For example, if Jane Smith requests her records from Peaceful Valley Hospital through a PHR that has verified her identity to NIST IAL 2 or 3, this request is regarded as being made directly from the patient and therefore requires no expiration date. This extends to PHR and medical/consumer hardware as well as software/systems that may be set by the user to make periodic requests for and/or to transmit data. The PHR or device in this case is a mechanism to make and receive the request that the patient themselves operates. This differs from the requests made by an insurer or other third party, which while made on the patient's behalf, are not a direct request by the patient and the patient is not the direct recipient of any of the data gathered.

### 4.4.2. Requirements for Query Responders

Query Responders are permitted to make access denial decisions based on the Initiator's Permitted Purpose as well as by the Access Policy Assertion they assert. If the Query Responder finds that its access policies allowing the release of records have not been satisfied by internal action, such as by collection of a form that generally authorizes such releases, and are not satisfied by the combination of the Query Initiator's Permitted Purpose and any Access Policy Assertions included with the query, it may indicate to the Query Initiator which of the Carequality Policy Assertions, if any, would allow access to the identified patient's records, using the technical approach described in the relevant Use Case Implementation Guide.

If the Query Responder indicates that one or more Policy Assertions would allow access to a patient's records, and the Query Initiator completes the requirements for the relevant Policy Assertion(s) and includes the Policy Assertion(s) in a subsequent request for that patient's records, the Query Responder must provide access to the records unless there has been a change to the patient's record in the meantime such that the particular Policy Assertion(s) no longer satisfy the Query Responder's access policies. It is expected that such an occurrence would generally be rare, and that Query Responders must generally release records if a Query Initiator asserts a Policy

Assertion that the Query Responder recently indicated would allow access to these records. If the Query Responder has received an "opt-out from exchange" by the patient or the patient's personal representative, this should override any Patient Permission assertion from a Query Initiator. Note that Query Initiators are under no obligation to attempt to comply with the requirements for the Query Responder's indicated Policy Assertion(s), or to attempt a follow-up request asserting such Policy Assertion(s). See Section 4.4.3 for more details on Error Responses for Access Denials.

#### 4.4.2.1. Evaluating Policies Prior to Responding to Patient Discovery Queries

As long as the Query Responder supports a particular query's Permitted Purpose, i.e., in categories #2-4 listed in Section 4.4, Query Responders must perform patient matching based on a Patient Discovery query prior to responding, in the absence of any technical error. If a patient match is identified, the Query Responder must assess its access policies for that patient to determine if they have already been satisfied by the Query Responder's internal actions, for example by collecting a form authorizing the release of information. If this assessment reveals access policy requirements that are still outstanding, the Query Responder must then assess any Carequality Access Policy Assertions made by the Query Initiator, to see if they satisfy the outstanding requirements.

#### 4.4.2.2. Patient Discovery Queries and Revealing the Existence of Records

Absent specific permission, Query Responders are permitted to never release information for a supported specific Permitted Purpose or to refuse to release information, including the fact that a record exists. However, the practice of an Implementer or CC refusing in their response to disclose that a matching record exists is discouraged, to the extent the disclosure is allowed by HIPAA, for all Implementers and CCs that are not substance abuse treatment facilities covered under 42 CFR Part 2, or other mental and behavioral health facilities that have significant restrictions placed on their release of information under Applicable Law.

#### 4.4.2.3. Unsolicited or Unsupported Assertions

Query Responders must be prepared to receive any Carequality Access Policy Assertions in such a way that does not negatively impact their system or workflow. This includes those policy assertions that are not utilized by the Query Responder. In these instances, Carequality Access Policy Assertions that are not relevant to the Implementer's access policy must simply be ignored by the Implementer.

With respect to unsolicited Policy Assertions from the Query Initiator, Query Responders are not required to consider them sufficient to satisfy local access policies.

> For example, suppose that Peaceful Valley Hospital has a record for John Smith. Peaceful Valley Hospital has been queried for this record by physician practice Adventist Medical. Adventist Medical (Query Initiator) asserts that they have satisfied the requirements of the Verbal Consent policy. Peaceful Valley does not utilize Verbal Consent as a factor within their access policy decisions. Receiving this assertion must not negatively impact Peaceful Valley's system or workflow.

#### 4.4.2.4. Reliance on Prior Policy Assertions

Query Responders must not rely on Carequality Access Policy Assertions previously asserted by the Query Initiator, i.e., should not "cache" policy assertions. Query Initiators are required to assert any Access Policy Assertions for which they meet the requirements with each transaction, and Query Responders should assume that if a Policy Assertion is not present in a transaction, it does not apply.

#### 4.4.2.5. Non-Discrimination With Respect to Policy Assertion Acceptance

If a Query Responder will accept a particular Policy Assertion(s) from one Query Initiator, it must accept that Policy Assertion(s) from any other Query Initiator for the same Permitted Purpose. This requirement applies equally to unsolicited Policy Assertions from the Query Initiator and to those assertions made after the Query Responder has indicated which Policy Assertions would satisfy its access requirements. Note that this requirement specifically applies to assertions made in the Access Consent Policy (ACP) field as defined by the relevant Implementation Guide.

> For example, suppose that Peaceful Valley Hospital has a record for John Smith. Peaceful Valley Hospital has been queried for this record by physician practices Adventist Medical and Children First. If Adventist Medical asserts that it meets the requirements of the Verbal Consent policy, and Peaceful Valley considers this assertion from Adventist Medical to satisfy its access policies for John Smith, then non-discrimination requires that it must also consider a Verbal Consent assertion from Children First to satisfy its access policies.

#### 4.4.2.6. Non-Discrimination With Respect to Access Policies

Query Responders are prohibited from enforcing different access policies based on attributes of the organization making the request. Stated differently, if a Query Initiator can legitimately claim a particular Permitted Purpose, the Query Responder must treat the request the same as any other for that Permitted Purpose, regardless of the Query Initiator's organization type or other attributes. Note that this requirement relates to the access policy itself, not necessarily to the outcomes of evaluating that access policy. Also note that this requirement refers to general access policies set by the organization, and does not prevent a Query Responder from honoring an individual patient's wishes to restrict release of his or her records to particular organizations.

Similarly, a Query Responder can't waive access policy requirements for a particular Query Initiator, or enforce additional access policy requirements for a particular Query Initiator.

> For example, suppose that Peaceful Valley Hospital has a record for John Smith. Peaceful Valley Hospital has been queried for this record by radiology practice Adventist Radiology and Children First Orthopedics. If Adventist and Children First are both querying for Treatment, non-discrimination requires that these two practices should have equal access to Mr. Smith's information. While Mr. Smith may authorize release to a specific practice, Peaceful Valley may not have an overall policy that treats the two organization types (e.g., radiology) differently.

It may be the case, however, that a Query Responder has an understanding – formal or informal – with a specific Query Initiator such that internal processes and workflows will result in access policy requirements being met for that Query Initiator.

> For example, Peaceful Valley Hospital and Children First may have developed a shared intake form for all patients that provides permission for the free release of records between the two organizations that is collected from all patients upon initial registration. Despite this arrangement, if Peaceful Valley's access policy requires Query Initiators to assert that a patient has provided consent, they must apply this standard to all Query Initiators equally.

Notwithstanding the previous requirement, Implementers or CCs that comprise the same business entity, for example a health system that uses two electronic health record systems that are connected via the Carequality Framework, may enforce different access policy requirements for responses to internal queries as opposed to those queries from external entities. Queries between two agencies of the federal government, or two agencies of a particular state government, also fall under this exception, with queries between government agencies being considered "internal" for purposes of this requirement.

#### 4.4.2.7. Policies Relating to Individual Users and Implications for Patient Restrictions

Query Responders are also prohibited from restricting access based on the role (occupation, title, etc.) of the individual user initiating a request. Conclusions about the individuals who ultimately will have access to see and use information that is released cannot reasonably be made in many cases based on the individual associated with a request. It is commonplace for non-clinical staff or the system itself to initiate requests so that information is available to actual clinical users. Conversely, even if a clinical user is associated with the request, the Query Responder cannot be certain that other users won't have access to the data in the requesting system once it is released.

Similarly, Query Responders should not base access policy decisions on the User Authentication Context Field or as defined by the relevant Implementation Guide for an inbound message. The accuracy and consistency of this value is currently questionable in practice. Carequality may permit the use of this field for access policy decisions in the future, if its use becomes more consistent across implementations. If this field is supported for a particular Use Case, details around its usage will be denoted in the relevant Implementation Guide

Given these limitations on the access restrictions that can be supported within the Carequality Framework, the practical outcome is that some patient requests for restrictions on releases must be regarded as an opt-out by the patient with respect to exchange via the Carequality Framework. Note that organizations can choose to honor patient requests regarding which individual organizations may or may not receive their information, as well as the Carequality Permitted Purpose(s) for which their information may be released.

The Query Responder should ensure that any permissions received from the patient or representative accurately reflect the requesting organization as identified by the Home Community Identifier in the query transaction. Query Responders should assume that any information released

in response to a query asserting that the Query Initiator can accept information from a facility covered under 42 CFR Part 2 may be accessed by users within the entire requesting entity identified in the Carequality Directory by the Home Community Identifier used in the query transactions. Information related to treatment in a facility covered under 42 CFR Part 2 should not be released if permission has not been given for the entire querying entity.

#### 4.4.3. Error Responses for Access Denials

Each Use Case Implementation Guide outlines possible error responses that Query Responders may employ when responding to an incoming query for which access has been denied in whole or in part. In instances in which error responses are appropriate, Query Responders must err on the side of providing the maximum information possible about the source of the error, while also limiting potential disclosures of patient data. While the most detailed available response is encouraged, Query Responders are not required to include detailed information in their error responses and may respond with an error code indicating no matching patient was found, even if a patient match was in fact found, if the Query Responder is unable to release any information about that patient to the Query Initiator, including even the fact that the Query Responder has a record for that patient. If this field is supported for a particular Use Case, details around its usage will be denoted in the relevant Implementation Guide.

> For example, suppose that Peaceful Valley Hospital has a record for John Smith. Peaceful Valley Hospital has been queried for this record by Adventist Medical. Peaceful Valley first performs a patient match based on the details provided by Adventist. Mr. Smith's record is found, however, due to Peaceful Valley's policies, patient records may not be shared without a signed policy assertion. In this instance, Peaceful Valley is encouraged to provide as much detailed information in their access denial response as possible to inform Adventist staff about what additional documentation is required.

### 4.5. Record Locator Services

A Record Locator Service provides a value-added service that makes querying for records easier and more efficient, but it is not required in order to obtain records since the record holder can be queried directly. A Record Locator Service provides the locations of patient records, but does not provide the records themselves or the clinical data they contain, which are requested from an Implementer or CC in the Query Responder role based on the locations reported by the Record Locator Service.

An Implementer or CC that is a Record Locator Service may honor patient location queries selectively based on additional agreements and charge a fee, including for patient location queries that are for Treatment. If supported for a particular Use Case, additional details regarding Record Locator Services will be denoted in the relevant Implementation Guide.

## 5.0 Performance Measures

In order to gauge Carequality's success in advancing widespread interoperability, Carequality may collect information from Implementers on a number of performance measures. Implementers shall

adhere to any and all statistic and Performance Measure reporting requirements defined for the Use Case(s) in which they participate. Failure to report these statistics in a timely manner, as defined by the Use Case, may result in punitive actions from Carequality, which may include, but are not limited to, a denial of access to Carequality Directory read/write privileges.

These measures are meant to quantify the impact of Carequality for a particular Use Case, not to evaluate individual Implementers, and the numeric value of the metrics themselves will have no impact on an Implementer's Carequality Connected status. If required for a particular Use Case, additional details regarding Performance Measures will be denoted in the relevant Implementation Guide.

# 6.0 Evidence of Compliance

Applicants wishing to become Implementers of a particular Use Case must show evidence that they are able to comply with the requirements of that Use Case. Implementers are subject to the testing and connectivity policies listed in the relevant Implementation Guide until a transaction testing process is described by Carequality. Implementers are required to follow any and all requirements mandated by the transaction testing program at that time.

Generally, applicant requirements fall broadly into two categories:

1. The Carequality Application Process as defined for all Implementers and CCs, regardless of Use Case.

2. Compliance of the Implementer's system(s) with the technical specifications of the role or roles that it or its CCs will play, or in the case of ongoing connectivity verification, do play.

If required for a particular Use Case, additional details regarding evidence of compliance will be denoted in the relevant Implementation Guide.

# 7.0 Directory Requirements

Implementers and their CCs must abide by the rules/policies that are outlined in the Carequality Directory Implementation Guide. Implementers that plan a significant restructure (i.e. changes to already published endpoints, OIDs, or other changes that impact the Implementer community's ability to exchange with the Implementer) to their gateway(s) MUST communicate their intent to Carequality. Implementers SHALL provide a written notice via email to admin@carequality.org at least 20 business days before the proposed changes are to be made. The written notice via email should include the proposed changes, must include a coordination/communication plan to inform the broader Carequality Implementer community, and must be reviewed and agreed to by Carequality staff.

In addition to the above, the following conformance statements MUST be adhered to:

- Test and Dev entries must not exist in the Prod Directory.

- Carequality Implementers must share Prod security information only with persons who need to know.
- Implementers must successfully pass the testing requirements as outlined in the respective Implementation Guide they are participating in before publishing entries for that Use Case.
- Implementers must successfully install their production Cert before being issued Prod security information.
- Implementers must adhere to field-level requirements reflected in the Use Case(s) Implementation Guide for Directory entry publications.