carequality

703-398-0960 | https://join.me/carequality

Carequality Patient Authorization Policy Workgroup Draft Conclusions

November 2, 2016

Background

The Patient Authorization Policy workgroup develops policy around the optionality of the patient authorization structure, authorization as it pertains to the non-discrimination principle, and the scope of authorization in patient discovery transactions. The following slides show the draft conclusions reached by the Policy Workgroup so far. These conclusions will be reflected in proposed updates to the Query-Based Document Exchange section of the Implementation Guide.

Draft Conclusions

- *A Query Responder is permitted to never release information (via Carequality) for a specific Permitted Purpose.*
- *A Query Responder may refuse to release information for a supported Permitted Purpose until they receive a specific authorization for that disclosure.*
  - *This is permitted, especially for Part 2 facilities*
  - *A statement in the implementation guide that discourages implementers from taking this option, unless legally obligated to do so, should be drafted. The statement will potentially make specific reference to 42 CFR Part 2.*
- *Query Responders are prohibited from enforcing different access policies based on the type of organization making the request.*
  - *Note that it IS allowed, and expected, for Query Responders to have different policies based on the Permitted Purpose*
  - *Since some types of organizations are inherently limited in the purpose they can legitimately claim, from a user perspective it may appear that there is a difference based on type of organization, when in reality the difference lies in the Permitted Purpose*
- *Query Responders are prohibited from restricting access based on the role (occupation, title, etc.) of the specific individual user initiating a request.*

Draft Conclusions Continued

- *Within the data exchange of query responders: If a Carequality Connection has an arrangement – formal or otherwise – with another organization that results in authorization requirements being met for releases to that organization, (Ex. based on a shared patient release form at intake) that arrangement is permitted as long as other, similar organizations who are willing to comply with the relevant terms are allowed to reach an appropriately similar arrangement.*
- *Organizations with several internal EHRs that allow the free flow of information for all permitted purposes between their organization's systems **CAN** require specific authorization to release records in response to any external query. This is not regarded as a discriminatory practice against the external organizations.*
- *Practical limitations dictate that many patient-based requests for restrictions on releases can't be supported through Carequality and must be regarded as an opt-out from Carequality.*
  - *Exceptions: Patients can specify individual organizations that may, or may not, receive their information as well as the purpose of use for which their data is being used.*
- *Information included with error code responses should err on the side of providing the most information possible about the source of the error, while also limiting the potential disclosure of patient data.*
- *The inclusion of detailed information within error responses is optional.*

Draft Conclusions Continued II

- *We want to continue to respect local autonomy, as a priority. Query responders should have significant leeway in determining access policies.*
  - *One specific corollary: Responders are not required to release patient information even if the initiator claims to have authorization.*
- *We should allow the Query Responder to indicate that authorization is needed, but requirements must be met out of band in instances where in-band technical support is unavailable. The idea is to provide an option for those organizations who want to provide more clarity in their responses, but aren't able (either from a technical or policy standpoint) to accept an assertion of authorization within a query.*
- *An initiator is not obligated to fulfill a responder's request for further authorization.*
- *A Query Responder* ***that supports an Initiator's permitted purpose for query*** *should perform patient matching based on that Initiator's request and assess the access policies involved for any specific, matching patient(s) before determining how to respond.*
  - *Note that a Responder may still provide a generic response including reporting that no matching patients were found, if their access policy prohibits revealing that the patient has a record*

Draft Conclusions Continued III

- *Requesters can assert compliance with any particular defined policies*
- *Responders can indicate that compliance with a particular defined policy OID is required for information to be released for a particular patient.*
- *If a particular policy **must always** be fulfilled for an Implementer or CC to release information (e.g. in the case of a "part 2 facility"), that fact must be made known to other participants, likely in the Carequality Directory*
- *Implementers should be prepared to receive **any** Carequality OlD in such a way that does not negatively impact their system or workflow. This INCLUDES those OIDs that are not utilized by the specific Implementer; OIDs that are not relevant to the Implementer's access policy should be simply ignored.*
- *The Initiator is responsible for the thorough and accurate documentation of signatures and forms they collect as well as the preservation of these documents for all OIDs they assert. These documents must be made available to the Query Responder in a timely manner.*

Draft Conclusions Continued IV

- *The Signed Document OID should be separated into four distinct OIDs:*
  1. *I have collected the Query Responder's form, and it is accessible within the transaction flow*
  2. *I have collected the Query Responder's form, but it is not currently accessible*
  3. *I have collected my form that includes the to-be-defined Carequality required elements, and it is accessible within the transaction flow*
  4. *I have collected my form that includes the to-be-defined…elements, but it is not currently accessible*
- *In addition to the Signed Document OID(s), there should be an OID that asserts that the Query Initiator has verbal consent to obtain records.*

Draft Conclusions Continued V

- *Query Responders should not cache previously asserted OIDs. Query Initiators should always assert any applicable OIDs and should not assume that the Query Responder will "remember" anything.*
- *Query Initiators should not assert policy OIDs related to having a signed form, unless that form will remain valid for at least 24 hours after the assertion is made*
- The emergency and public health disaster concepts should be conveyed using policy OIDs, not by new permitted purposes. These concepts describe particular circumstances under a broader permitted purpose, such as Treatment or Public Health, not separate purposes.
- Data shared under emergency situations generally does not need to be handled different than other patient data. If it's sensitive otherwise, it's still sensitive, and if it wasn't, it still isn't.
- Query Responders may assert the Public Health Disaster OID when a request is associated with an officially declared state or federal disaster.
- A baseline definition of "emergency" should be established by Carequality – perhaps modeled on 42 CFR Part II's definition
- Initiators who assert the Emergency policy OID must comply with reasonable follow-up requests from the Query Responder in order to comply with the Responder's regulatory obligations (e.g. collecting a signed form after the fact, or providing info on the nature of the emergency)

Draft Conclusions Continued VI

- Carequality will define a mapping of Permitted Purposes from a policy standpoint into PurposeOfUse values from a technical standpoint
- Carequality Implementers' use of legal proxies for the patient (i.e. authorized individuals such as family) may be noted, but should be functionally treated as if the patient has made the request. The Query Initiator is responsible for ensuring that these proxies are in fact authorized and appropriate to make requests as defined by HIPAA.
- Carequality Query Responders should not make access control decisions based on the User Authentication field.
  - The accuracy of this value in the field is currently questionable. The value is prone to errors and is therefore not appropriate to consider in access control determinations
  - Query Initiators should provide meaningful requester verification information as well as comply with all HIPAA authentication standards.
- We will not define a policy OID for IAL 1; no use case in which this level would be accepted was presented.
- A statement should be added to the IG that Query Initiators that choose to assert IAL 2-3 through a trusted registration authority (third party), is also responsible for validating that third party's verification process.

Draft Conclusions Continued VII

- There should not be separate OIDs for each trusted registration authority. Query Initiators should only assert the IAL that they comply with.
- Elements required for the policy OID stating that the requester has collected an authorization form that meets Carequality standards, will be the elements required by HIPAA for authorization forms, without any additions.
- Carequality will define a policy OID that asserts that the requesting organization is able to appropriately handle “Part 2” data
- The policy OID for Part 2 data handling will be accompanied by document metadata identifying a document as containing “Part 2” data
- In order to better frame the use of “Part 2” data, we will draft policy requirements that both
  - Communicate the fact that Part 2 data is being released to the receiving party, in a way that can be reasonably interpreted by the receiving party

  AND
  - Allow the sending organization to rely on the fact that information will not be disclosed beyond the requesting organization as that requesting organization is specifically identified in the query
- In cases where NIST Identity Assurance Level 3 requirements are met, sending policy OIDs for both level 2 & 3 is required (note: if you meet the IAL 3 requirements, you also meet the IAL 2 requirements)
- The Policy OIDs for IAL Verification should be split into two distinct classes, one for the patient themselves, and one for the patient’s legally authorized proxy.

Thank You!