Carequality Principles of Trust

Ratified Jan, 2015

TABLE OF CONTENTS

1 INTRODUCTION

Technology has evolved to the point that widespread electronic exchange of health information is possible. Health care providers seeking to demonstrate "meaningful use" under ARRA, patients seeking to have all of their medical information conveniently available, accountable care organizations seeking to promote care coordination, and many other applications are valuable uses of electronic health information exchange. To realize this value, many health information exchange (HIE) networks have developed over the past ten years. These HIE networks vary in size, scope and level of participation. Some are smaller, local HIE networks in which a hospital system and its community physicians participate. Some are regional networks encompassing otherwise competing hospital systems and physicians. A few large-scale, nationwide networks have emerged that seek to connect the smaller HIE networks, allowing them to interoperate and exchange information across networks. Most notably, the eHealth Exchange has emerged as a nationwide HIE network as have some electronic health record vendor networks. We are now at a point where these large, nationwide networks want to enable exchange by and among their users to truly allow for seamless nationwide health information exchange. To do this, however, the networks must reach consensus on the implementation specifications and business rules that will govern their relationships. The development of this consensus is the focus of the Carequality initiative.

2 CAREQUALITY OVERVIEW

The Department of Health and Human Services (HHS) has identified "interoperability" of electronic health records as a significant challenge and has encouraged the health information technology industry and health care providers to work collaboratively to address this challenge so that the Federal government would not have to undertake the long and arduous process of regulation. In response, health care providers and key health IT vendors decided to jointly undertake this work. Given its successful work with the eHealth Exchange, they asked that The Sequoia Project serve as the convener of this effort, which The Sequoia Project Board of Directors approved in February 2014. The initiative, called Carequality, is dedicated to accelerating progress in health data exchange among multi-platform networks, health care providers, payers, and EHR and HIE vendors. The Sequoia Project's goal with the Carequality initiative is to facilitate agreement on a common national-level set of technical and business requirements that will enable providers to access patient data from other groups as easily and securely as today's bank customers connect to disparate banks and user accounts on the ATM network. Once achieved,

this level of health data interoperability will represent a quantum leap in the quality of health care available and reduce the cost to support interoperability.

Carequality functions as a distinct initiative of The Sequoia Project. The Sequoia Project serves as the convener for Carequality and provides it with a corporate home for legal and contractual purposes, as well as staffing, administrative support, communications and outreach, and other roles as needed to support Carequality. The Sequoia Project Board of Directors recognizes that addressing the interoperability challenge will require a significant amount of oversight so it has appointed a Steering Committee to provide this oversight. Within the limits of its charter, the Carequality Steering Committee will govern all Carequality activities (including the Trust Framework Work Group activities) and the implementation of the Carequality Implementation Guides by the Carequality Implementers. The Carequality Steering Committee will have the ability to adopt the Implementation Guides, as well as any other documents that are necessary to memorialize the Trust Framework.

Carequality is an open, transparent, inclusive, industry-driven effort that will convene stakeholders and facilitate consensus to develop and maintain a standards-based interoperability framework that enables information exchange between and among "Carequality Implementers" and their customers. Carequality Implementers are networks and service providers that have implemented and have been verified as complying with a Carequality Implementation Guide. The term "networks" is construed very broadly to include health information exchange organizations (HIOs), federated nationwide networks like eHealth Exchange, and commercial health information exchange networks (e.g. Commonwell, e-prescribing networks, release of information companies, EHR vendor networks). The term "service provider" is intended to include providers of services used by networks in the conduct of HIE. Services may include capabilities, such as provider directories, that are hosted and maintained by a service provider and used by networks to locate and/or identify providers, or to record locator services that are used by networks to identify locations of patient records. Each Implementation Guide will include a description of the Use Case as well as the applicable implementation technical requirements (specifications and testing), business requirements and policies that support the trusted exchange of data among Carequality Implementers.

Carequality's implementation guide focused work will begin with a Use Case related to query for information, both with and without a Record Locator Service, and may be broadened to include other capabilities over time (e.g. Provider Directory, etc.). For each Implementation Guide, Carequality will appoint a specific Work Group whose mission is to accommodate and build upon existing approaches for that particular Use Case or capability; assess requirements for bridging between existing approaches; and, reach consensus on implementation specifications, business requirements and policies for this bridging. The consensus decisions of each Work

Group will be documented in final Implementation Guides that will be approved by the Carequality Steering Committee.

3 The Role of the Trust Framework Work Group

For the past ten years, many involved in health information exchange have been talking about the role of trust and interoperability in data exchange networks. The reality is that while these discussions have been occurring, there is no uniform agreement on what trust means, the role trust should play and, indeed, whether trust is even required in order for parties to be willing to exchange data. Even where there is agreement that trust is important, there are material differences in the way in which different networks define, establish and maintain trust. These differences take the form of operational policies and technical rules that vary across networks. As a result, parties often have to negotiate the terms of trust before they begin exchanging. This is done at the provider-to-provider level, the provider-to-network level and the network-to-network level. Carequality has recognized that this perceived need for negotiations is a barrier to achieving all of the value associated with robust health information exchange and is seeking to remove this barrier by developing industry-led consensus Implementation Guides that are based upon a flexible and scalable trust framework. The Carequality Implementers who choose to comply with a specific Implementation Guide will be able to interoperate with each other and exchange information on behalf of their customers without the need for any additional negotiations or documentation of technical or business requirements or legal relationships.

The Carequality Steering Committee tasked the Trust Framework Work Group with developing "Principles of Trust" for Carequality that will serve to establish trust between Carequality Implementers to enable the electronic exchange of health information and as the uniform guide for the development of the implementation specifications, business requirements and policies that will be documented in each Implementation Guide. The Principles of Trust should have the following characteristics:

- **Flexible:** The Principles must be adaptable to many different types of organizations and business models since there is a great variety of both involved in Carequality.
- **Scalable**: The Principles cannot require a complex administrative infrastructure in order to function since this will add cost and impede the goals of Carequality.
- **Implementable**: The Principles must be able to be implemented by organizations with differing financial and technical resources.
- **Promote consistency**: The Principles must provide a consistent model for behavior that is clear to all Implementers.

- **Enforceable**: The Principles must be enforceable by a mechanism established by the Carequality Steering Committee so that all parties understand that there are consequences for failing to comply.[1]

It is not possible to create a single, comprehensive set of Principles of Trust that apply to every model of data exchange. For that reason, the Trust Framework Work Group has identified two types of principles – Universal and Customizable.

Universal: There will be certain principles that apply in the same way to all Carequality Implementers for all Use Cases and Implementation Guides. In other words, the trust principle and the implementation of that principle will be the same for the Query/Retrieve Use Case as for another Use Case (e.g. Provider Directory, etc.). For instance, all Carequality Implementers must comply with HIPAA. Compliance with HIPAA is required regardless of the Use Case or type of Carequality Implementer. These principles are referred to as "Universal Principles of Trust." A single set of policies addressing compliance with the Universal Principles of Trust will be developed and incorporated by reference into each Implementation Guide.

Customizable: There will be certain principles that apply generally to all Carequality Implementers for all Use Cases, but the specific application of which will vary with the Use Case. These principles are referred to as the "Customizable Principles of Trust." For instance, all Use Cases will have to specify the purposes for which the Use Case can be used, but these purposes may differ between the Query/Retrieve Use Case and the Provider Directory Use Case. Each Use Case Work Group will be tasked with tailoring the Customizable Principles of Trust for its specific Use Case and documenting this customization in the applicable Implementation Guide.

The Trust Framework Work Group believes that most of the principles should be Universal Principles of Trust so that each Use Case Work Group has definitive guidance on how to design the implementation specifications, business requirements and policies for each Use Case. This will also minimize the burden on future Use Case Work Groups and the amount of work that must be done to stand-up a new Use Case. The Use Case Work Groups will only have to focus on describing the way in which they will define the Customizable Principles of Trust to address issues that are unique to its specific Use Case.

[1] While all of the Principles of Trust should be enforceable, the Trust Framework Work Group is not tasked with identifying or implementing the enforcement mechanisms. The Carequality Steering Committee will develop a mechanism to hold Carequality Implementers accountable for compliance with and to enforce the Principles of Trust.

As with all Carequality activities, the Trust Framework Work Group used an open, transparent, inclusive, public-private, consensus based approach to develop the Principles of Trust. This document sets forth Universal and Customizable Principles of Trust for the Trust Framework Work Group's consideration. The Trust Framework Work Group worked collaboratively to review and refine these Principles of Trust and arrive at consensus on the final Framework. The Work Group has reached consensus and is presenting the Trust Framework to the Carequality Steering Committee for approval.

4 UNIVERSAL PRINCIPLES OF TRUST

There are some principles of trust that must be present in every health information exchange relationship and service whether it is point-to-point, a network, or a network of networks and whether the Use Case is query/retrieve, push, publish/subscribe, or record locator service. These principles are so foundational to the trust among exchange partners and service providers that many times they are implicit or assumed. For Carequality Implementers, it is important that these foundational Universal Principles of Trust be explicitly acknowledged to provide comfort to both the Implementers and their customers across all Use Cases. These Universal Principles of Trust are described below.

1. ***HIPAA Compliance – Carequality Implementers will protect the privacy and security of information exchanged through their networks or using their services by adopting, at a minimum, the HIPAA privacy and security standards.*** Protecting the privacy and security of information exchanged through use of the Carequality Implementation Guides is of paramount importance. To help ensure that Carequality Implementers do this, each Carequality Implementer must at least comply with the Health Insurance Portability and Accountability Act ("HIPAA") privacy and security standards for all data exchanged through its network or by use of its service. Carequality Implementers might also be subject to state data privacy laws, or to federal laws other than HIPAA that require them to have privacy and security measures that are more protective than those required by HIPAA. In those cases, the Implementer must comply with those applicable laws. For many Carequality Implementers compliance with HIPAA is simply a restatement and affirmation of its existing legal obligations as a business associate of covered entities or as a covered entity itself. For some, however, compliance with HIPAA may be a new requirement. Carequality believes that imposing such a new requirement on a Carequality Implementer is important to establish consistency among all Carequality Implementers and to establish a generally accepted baseline for the protection of health information. To achieve the goals of Carequality, Carequality Implementers and their customers must be willing to interoperate with each other based solely on the fact that the other party is or is associated with a Carequality Implementer. Having a universally

recognized baseline for privacy and security is one part of the trust framework that will support this.

- Example 1: A Carequality Implementer that is an information exchange network is most likely a business associate of its covered entity customers. As a result, it is required to comply with HIPAA. This Principle simply reinforces that requirement but does not expand it.
- Example 2: Certain Personal Health Records vendors are not covered entities or business associates under HIPAA. Moreover, they may not be required by state law to protect the privacy and security of the information they maintain on behalf of their customers. If these PHR vendors choose to become Carequality Implementers, then they must comply with the HIPAA Privacy and Security Rules as if they were a business associate.
- Example 3: Social Security Administration (SSA) is not a covered entity or business associate under HIPAA. Instead, SSA is required to comply with FISMA and other applicable federal privacy laws that are arguably more stringent than HIPAA. This Principle requires Implementers to comply with HIPAA as a *minimum* requirement. Since SSA is already subject to stricter laws than HIPAA, they would be required to comply with these applicable federal laws as a Carequality Implementer.
- Example 4: Implementer A, a Texas based organization, queries for information from a Implementer B, a California organization. Implementer A is governed by Texas law so it will need to ensure that its query, and its use of any information that it receives in response to the query, is handled consistent with Texas privacy law to the extent that Texas law is not preempted by HIPAA. Implementer B is governed by California law so it will need to ensure that its response to the query is handled in a manner that is consistent with California law to the extent that California law is not preempted by HIPAA. The fact that Implementer A and B are both Carequality Implementers will not cause either of them to be subject to the other's state law.

2. ***Compliance with Implementation Guide for a Use Case – Carequality Implementers will, to the extent not prohibited under applicable law, implement all mandatory aspects of the Implementation Guide for a Use Case***. Each final Implementation Guide that is approved by the Carequality Steering Committee will contain a number of components including policies, procedures, technical requirements (implementation specifications and testing), business requirements, or service level agreements (SLAs). Carequality is a diverse community. Some Implementers are data sharing networks, some are technology vendors that only license software to customers and still others are governmental agencies. The Implementation Guide will take this diversity into account and will indicate which components are applicable to all Carequality Implementers of that Use Case and which components will vary based on the role that the Implementer plays in the Use Case

(see Customizable Principle of Trust #3). In order to provide some degree of flexibility, the Implementation Guide will indicate which of the components are mandatory for an Implementer and which are strongly recommended but are not mandatory. An Implementer must comply with components of the Implementation Guide that are mandatory and that apply to their particular role or use. The only exception to this requirement will be if compliance with a mandatory component of the Implementation Guide would cause the Implementer to violate its applicable law. This is important to prevent Implementers from selectively implementing components of an Implementation Guide that everyone else is expected to follow since that will create uncertainty among Implementers about what components are actually being followed. This uncertainty would inhibit full interoperability.

- Example 1: The Implementation Guide for the Query/Retrieve Use Case will need to recognize that some Carequality Implementers will only request information and never provide information. The Social Security Administration is a good example of this since SSA will participate in this Use Case to obtain information about persons who have applied for disability; however, SSA will never respond to requests for information. The Implementation Guide will identify which components apply to Implementers that only request information and these organizations will not be required to comply with the Implementation Guide components that apply to those who respond to requests for information. Implementers who function in a "responder only" role would be required to comply with all of the components of the Implementation Guide applicable to "responders," but would not be required to comply with the components applicable to "initiators."
- Example 2: The Implementation Guide for the Query/Retrieve Use Case might include specific requirements for patient matching. The Query/Retrieve Work Group will determine whether these requirements are mandatory or suggested and which Implementers the requirements apply to, e.g. initiators only, responders only, both. If the requirements are mandatory for responders, then every Carequality Implementer with the role of responder is required to comply with the patient matching requirement unless doing so is prohibited by applicable law.
- Example 3: The Query/Retrieve Use Case is likely to have mandatory and suggested components that will vary based on the role that the Implementer decides to implement, e.g. initiator, responder, both. An organization would be allowed to become an Implementer for one role and then add more roles later.

3. ***Non-Discrimination – Carequality Implementers will promote interoperability by not discriminating against other Carequality Implementers.*** Carequality's goal is to enhance and enable interoperability by reducing the technical and policy barriers that exist today. This goal cannot be realized if Implementers selectively restrict interoperability with other Implementers even though they comply with all of the mandatory requirements of the

Implementation Guide that apply to them. All Carequality Implementers 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 that have implemented the mandatory requirements of the same Implementation Guide. By agreeing to become a Carequality Implementer, an organization is agreeing to treat equally all other Implementers that are similarly situated.

- Example 1: A Carequality Implementer responds to authorization-based queries from SSA. The Implementer must respond to all valid authorization-based queries. It cannot choose to ignore authorization-based queries from other Carequality Implementers (e.g. payors, providers, ACOs).
- Example 2: Carequality Implementer A decides to not permit exchange with any Carequality Implementers that are part of a network using certain proprietary software. The two Carequality Implementers are technically interoperable because they have both implemented the same Implementation Guide and comply with all of the mandatory requirements, but Implementer A has chosen to not permit exchange with Implementers on the other network because Implementer A considers the other network to be a competitor. This type of restriction on interoperability is unfair and unreasonable and would therefore violate the Non-Discrimination Principle.
- Example 3: A Carequality Implementer allows its customers to interoperate and exchange information with each other without any additional legally binding arrangements. This same Implementer does require additional legal arrangements, above and beyond the Trust Principles, for interoperability and exchange of information between their customers and other Carequality Implementers. Requiring additional legal arrangements to interoperate and exchange information with other Carequality Implementers is unreasonable given that all Carequality Implementers will be bound to comply with the Trust Principles and Implementation Guides. As a result, enforcement of such a policy would violate the Non-Discrimination Principle.
- Example 4: Carequality Implementer A requests information from all other Implementers, except Implementers B and C. Implementer A does not request information from Implementers B and C because, while Implementers B and C comply with the mandatory requirements for a Use Case, Implementer A has determined that Implementers B and C simply do not have enough information to justify the request. This is a reasonable restriction to impose; therefore, Implementer A would not be violating the Non-Discrimination Principle.

4. ***Local Autonomy – Carequality Implementers will be able to honor their local rules so long as such rules are applied consistently and do not unfairly or unreasonably limit interoperability.*** Many Carequality Implementers have developed their own rules for the use of their networks or their services. In some cases, these rules were informed by a

consensus process that involved representational stakeholders. In other cases, these rules were developed by the Implementer without input from stakeholders. These local rules often result in a Carequality Implementer not being able to exchange with another Implementer even though the other Implementer complies with all of the mandatory requirements of a particular Use Case. This is problematic and does not advance Carequality's goal of promoting widespread interoperability. However, at least initially, an Implementer will be permitted to continue acting in accordance with these local rules provided that such rules are applied consistently with respect to other Implementers and do not impose unfair or unreasonable conditions that would limit interoperability or otherwise conflict with the Implementation Guides. For instance, a Carequality Implementer may have a local policy that it will not exchange information in response to a request where the purpose of the request is payment. So long as the Carequality Implementer never exchanges information in response to a request where the purpose of the request is payment and exchanging information for payment purposes is not part of "full" participation (see the Customizable Principles), the Implementer's local policy will be respected. The Implementer cannot, however, selectively respond to requests where the purpose is payment if the request is from a certain Implementer and not respond where the request is from another Implementer. This would be an inconsistent application of the Implementer's local policy and would unreasonably inhibit interoperability.

- Example 1: A Carequality Implementer has implemented a local rule that it will only respond to requests based on treatment as the permitted purpose. The Implementer believes that this rule is consistent with its applicable law. Assuming that the Implementer never responds to requests for any other permitted purpose, the Implementer is permitted to honor this rule as it is applied consistently and does not unreasonably limit interoperability.
- Example 2: Carequality Implementer A has implemented a local rule that it will only respond to requests from healthcare providers. This local rule is a policy decision that is not required by applicable law. If the Implementation Guide for a Use Case includes a mandatory requirement that Implementers respond to requests from Permitted Users and Permitted Users include more than just healthcare providers, the Implementer must comply with this mandatory requirement. It does not matter that the Carequality Implementer applies the "healthcare provider only" local rule consistently because the Implementation Guide has a mandatory requirement that defines Permitted Users more broadly.
- Example 3: A Carequality Implementer in Texas has established business rules that allow it to respond to requests from other Carequality Implementers that are in Texas, but prevent it from responding to requests from Carequality Implementers outside of Texas. These rules are based on compliance with Texas law and the assumption that Carequality Implementers within Texas are bound to comply with Texas law. Provided that the Carequality Implementer does not respond to any

requests from a Carequality Implementer outside of Texas, implementation of this business rule would not violate the Local Autonomy principle as the condition is a reasonable restriction to ensure compliance with applicable law.

- Example 4: A Carequality Implementer has implemented an "opt-in" policy for its network. This local rule is a policy decision that is not required by applicable law. This means that the Implementer will only release information in response to a request if the individual has "opted-in." While this policy may inhibit exchange to the extent that individuals have not opted-in, this is a reasonable business rule that is consistent with Local Autonomy.

5. ***Accountability – Each Carequality Implementer will be responsible and accountable for its own actions.*** Each Carequality Implementer is relying on all other Implementers to operate their networks, or provide their products, in a way that does not expose Implementers to risk for something that the Implementer cannot control. One way to address this to requiring each Carequality Implementer to accept responsibility and be accountable for its own actions in connection with the Use Cases and, if the Implementer operates a network, the actions of those who exchange information through the use of the Implementer's network . In cases where there are adverse events or a Carequality Implementer fails to comply with an Implementation Guide, accepting responsibility means answering for such adverse events or non-compliance. Answerability includes penalties for failing to uphold commitments to be a trusted Carequality Implementer and, if appropriate, redress for those harmed by such failure. A common desire to avoid these consequences and remain a trusted Carequality Implementer provides some comfort that all other Carequality Implementers will uphold their commitments to comply with the Implementation Guide. It is important to stress that a Carequality Implementer is only responsible for actions, or failures to act, by itself, by those within its network if the Implementer operates a network or by its customers only if the Implementer provides some service to the customer that would provide the Implementer with a means to monitor the customers exchange activities. It is not the intent of this principle to ask Carequality Implementers to assume risk for the actions of others over whom the Implementer has no ability to control or influence. The Implementer is free to decide what contractual provisions it has with its network or customers to allocate any risk associated with this principle to others within its network or with its customers. It is also important to note that being accountable to other Implementers implies having the financial resources to cover any damages that one causes. This could include having "cyber insurance" for data breach liability but that is not the only way that this could be addressed.

   - Example 1: In making an update to its system, a Carequality Implementer inadvertently implemented a modification that made it non-compliant with the specifications in the relevant Carequality Implementation Guide. This non-compliance led to a failure in interoperability with other Carequality Implementers. This failure in interoperability was brought to the attention of the

Implementer. The Implementer must remedy this non-compliance or cease being a "Carequality Implementer."

- Example 2: In making an update to its system, a Carequality Implementer modified its software, which resulted in an unintended overriding a component of a Use Case specification related to Permitted Users. As a result of the modification, the Implementer allowed persons within its network to initiate requests for information even though those persons did not meet the definition of a Permitted User for that Use Case. Other Implementers, relying on the accuracy of the request responded with information. The non-compliant Implementer will be responsible for damages associated with its non-compliance.
- Example 3: Carequality Implementer A's end-user uses Implementer A's network to obtain data from other Carequality Implementers for a malicious purpose in violation of the rules governing Implementer A's network. The other Carequality Implementers from whom data was obtained suffer damages as a result of Implementer A's end-user's actions. As between Implementer A and the other Carequality Implementers, Implementer A will be responsible for the damages incurred by other Carequality Implementers because it is operating the network that its end user used to perpetrate the harm. Implementer A is free to have in place legally enforceable agreements for its network that "flow down" this risk to the end-user.

6. ***Cooperation – Carequality Implementers will cooperate with each other on matters relating to interoperability and shared Use Cases.*** To help promote trust among Carequality Implementers, all Implementers will work together to achieve Carequality's goal of widespread interoperability. Each Carequality Implementer will cooperate with other Carequality Implementers with respect to issues associated with the Carequality Use Cases in which the Implementer participates. Cooperation includes: (i) notifying other Carequality Implementers if there is a technical difficulty that is prohibiting proper functioning of the Use Case and working cooperatively to resolve such difficulty; (ii) notifying other Carequality Implementers of any issues that could have a material adverse impact; (iii) responding in a timely manner to inquiries from other Carequality Implementers about possible issues; (iv) taking steps to assure that an Implementer's network members or customers cooperate with others around issues related to exchange of information; and, (v) agreeing to resolve disputes through a collaborative, collegial, peer review process instead of immediately resorting to legal proceedings.
   - Example 1: Carequality Implementer A begins receiving complaints from its end-users that Carequality Implementer B has stopped responding to requests. In the spirit of cooperation, Carequality Implementer A will reach out to the point of contact for Carequality Implementer B to notify Implementer B of the issue. Implementer B will work to identify the source of the issue and will work to resolve the issue so that it resumes responding to requests. To the extent that

Implementer A and B must work together to identify the source of the issue or the solution, they will do so in a cooperative manner.

- Example 2: The Steering Committee will develop a process by which Carequality Implementers will work together to resolve disputes that involve the interpretation of a Carequality Implementation Guide in a collaborative manner. Implementers might disagree about what a business requirement of an Implementation Guide means or how it should be made operational. This type of dispute should be resolved through open communication in which Implementers agree to participate.
- Example 3: There might be situations in which an Implementer believes that its business is being damaged because another Implementer is not complying with its obligations as a Carequality Implementer. Instead of initiating legal proceedings, Carequality Implementers will agree to participate in dispute resolution process in hopes of resolving the dispute.
- Example 4: Implementers agree that they will commit personnel and resources to work collaboratively to develop new specifications that advance interoperability instead of working in "silos." Some specifications that have been discussed relate to content and patient matching.

7. ***Acceptable Use – Carequality Implementers will only use the widespread interoperability that is available through use of the Implementation Guides for permitted purposes as defined in the Implementation Guides and on behalf of their customers.*** Compliance with the Implementation Guides will result in widespread interoperability. Given the value of the data that can be obtained through use of the interoperability, it is critical that Carequality Implementers be trusted to use this interoperability only for permitted purposes and only on behalf of their customers who have entrusted them with this data. Carequality Implementers will adopt specific measures to assure that this does occur. Specifically, if the Carequality Implementer is a business associate that is participating and exchanging data or providing services on behalf of covered entity clients, then it will only use such interoperability to transact information on behalf of its clients and not on its own behalf. In addition, the Implementer will not re-use or re-disclose such information independent of its customer or the rights granted by such customer. It will not aggregate, de-identify or sell any data passing through its system for its own benefit unless its customer has given it the explicit authority to do so.
    - Example 1: If the Carequality Implementer is an EHR vendor, the Implementer may not request information for its own purposes independent of a request initiated by its end-user customer. For instance, such a Carequality Implementer could not request data on individuals simply to build out its own data warehouse. It could only request data when such request was initiated by an end-user (assuming that the request is for a permitted purpose).

- Example 2: A Carequality Implementer end-user might want to take advantage of the increased interoperability to request records from many sources to create its own database for use with its analytics tools for population health. Unless this is a permitted purpose, the Implementer cannot allow this.
- Example 3: Today, in the world of paper exchanges, once an end-user receives information in response to a request, that information becomes part of the end-user's official records. The end-user is allowed to re-use and re-disclose that information in accordance with applicable law. This will continue to be true in the world of electronic exchange. The difference is that the end-user's official record may be hosted or maintained by a Carequality Implementer. The Acceptable Use Principle prevents the Carequality Implementer from using that official record, to which it has access, for any purpose or in any way unless authorized by the end-user.

8. ***Universal Customer Flow Downs – Carequality Implementers must ensure that their customers or network members agree to act in accordance with the applicable components of the Implementation Guides and have the ability to suspend or terminate those who fail to do so.*** The principles of trust and Implementation Guides apply primarily to Carequality Implementers and the way in which they conduct themselves. In many cases, however, the Implementers' customers or members of the Implementer's network will be the ones actually exchanging information. As a result, it is important that these customers be bound to act in a certain manner to ensure that the chain of trust is not broken. To that end, each Carequality Implementer will require its customers to agree to the following:
   - Permitted Purposes: Each Carequality Use Case Work Group will select from among a pre-determined list of acceptable Permitted Purposes the ones that are available for that Use Case (see Customizable Principle of Trust # 1). All Carequality Implementers that implement a Use Case will be required to take measures to require that its network members and customers agree to only use the Use Case for a Permitted Purpose. Carequality Implementers may permit their customers to use the Use Case for a more limited set of permitted purposes, but may not broaden the Use Case approved set of permitted purposes. For instance, if the permitted purposes for a Use Case are treatment, payment and operations, a customer could limit use to treatment only but could not expand the use to include research.
   - Cooperation: Just like the Implementer is required to cooperate with other Carequality Implementers with respect to a certain Use Case, an Implementer will require its customers or network members to cooperate with other Carequality Implementers and customers or network members of Implementers with respect to Use Cases.

- Non-Discrimination: Carequality Implementers must take steps to require that its customers or network members not discriminate against other Carequality Implementers, and their customers or network members, in using the Carequality Use Cases. Without this requirement, the Non-Discrimination Principle would have little practical effect.

Carequality will not mandate the way in which the Carequality Implementers impose these requirements. It can be accomplished through contracts, policy or any other mechanism chosen by the Carequality Implementer so long as the mechanism is legally binding on and enforceable against the customer.

Carequality Implementers will also have the ability to suspend or terminate a customer's ability to use the Implementer's Use Case services if the customer fails to comply with the above requirements or otherwise presents a risk to the privacy or security of information exchanged with other Carequality Implementers. For instance, if the Carequality Implementer has implemented the Query/Retrieve Use Case, the Implementer must have the ability to suspend or terminate the ability of a customer or network member to submit a query if that customer or network member poses a risk to the privacy or security of the Use Case or information exchanged using the Use Case. The Carequality Implementer will also be required to assure that its customers or network members have the ability to suspend or terminate the use of their systems by individual end users who act in a way that poses a risk to the privacy or security of the information being exchanged using a Use Case. Being able to remove a bad actor from the exchange of information through the Use Cases is critical to trust among Implementers and their customers.

9. ***Identity Proofing and Authentication – Carequality will adopt identity proofing and authentication requirements for all Implementers and will require Implementers to adopt measures that will ensure that only those who are allowed to access the Implementer's network or services do so.*** It is unrealistic to expect that parties will exchange information with just anyone. A party will only exchange information where it knows the party with whom it is exchanging data or where the party is confident that the other party is who he purports to be. In the Carequality Use Cases, given the nationwide scope of the project, those participating will likely not know each other. Instead, they will be relying on the Carequality Implementers to have confirmed the identity of those participating through its network or the use of its services. As a result, each Carequality Implementer will be required to only allow those customers, network members or end-users who have been authorized, identity proofed and authenticated to use the Carequality Implementer's Use Case services. Identity proofing and authentication may be done directly by the Carequality Implementer or the Carequality Implementer may delegate this function to a subcontractor or customer. Whether it is done directly or

indirectly, however, it must be done before customers or end-users are technically enabled to use the Carequality Implementer's service. An important corollary to this requirement is that any organization that becomes a Carequality Implementer must also be identity proofed and authenticated before being allowed to claim that they are an Implementer. The Steering Committee will determine the mechanism for identify proofing Implementers.

10. ***Information Handling Transparency – Carequality Implementers will make their information handling practices transparent and easily available to customers and the public.*** HIPAA requires covered entities to publish a Notice of Privacy Practices so that patients will understand the ways in which the covered entity may use or disclose the patients' protected health information. HIPAA does not, however, require business associates to publish a Notice of Privacy Practices. As a result, there is some concern that there is little transparency when it comes to the information handling practices of those involved in, or enabling, HIT. In an effort to raise the bar and promote trust, each Carequality Implementer will be required to make publicly available a statement of its information handling practices that will include an accurate and easy to understand description of the following: the type of information the Implementer collects; the types of uses and disclosures the Carequality Implementer makes in the routine course of business for each type of information that it collects; the information exchange networks in which it participates and the way in which it participates; any de-identification or aggregation of information that it performs and information about what is done with such de-identified or aggregated information; and the way in which a customer may restrict the Implementer's use, disclosure, de-identification, or aggregation of its information. To the extent that any Implementer or customer of an Implementer questions the veracity of statements included in an Implementer's statement of information handling practices, such questions will be resolved through the dispute resolution process or other enforcement mechanisms established by the Steering Committee.

5 CUSTOMIZABLE PRINCIPLES OF TRUST

There are some principles of trust that should be present in every health information exchange relationship and service, but the way in which the principle is implemented will vary across Carequality Implementation Guides. For these Customizable Principles of Trust, the Trust Framework will include a general description of the principle, but the Use Case Work Groups will have to determine how to customize the principle for its Use Case. The customized principle will then be approved by the Steering Committee and memorialized in the applicable Implementation Guide. These Customizable Principles of Trust are described below.

1. ***Permitted Purposes – Use Cases will only be used for certain permitted purposes.*** The primary goals of health information exchange networks and services are to improve the health of patients and the efficiencies of health care delivery. While those participating in HIE all share this common goal, they may desire to exchange information for a number of different purposes to reach this goal. Some of these purposes may be acceptable to all, while others may only be acceptable to a few. To ensure that expectations are clearly defined and that all Carequality Implementers understand for what reasons they can use an Implementation Guide, each Use Case Work Group will establish a list of specific "permitted purposes."
2. ***Permitted Users – Carequality Implementers will only allow permitted users to use their Use Case services.*** A code of conduct for health information exchange should not only describe what is expected of the participants regarding their health information exchange activities, but should also specifically identify the types of entities and individuals that will be allowed to participate in the health information exchange activity. These are the Permitted Users. By identifying the types of Permitted Users, the network can help ensure that only those who need to exchange information for legitimate purposes, and who have been identity proofed and authenticated, will be allowed to do so. This restricted access to the network engenders trust. To ensure that expectations are clearly defined and that all Carequality Implementers understand what types of organizations and individuals can use a Use Case, each Use Case Work Group will establish a list of specific "Permitted Users." Each Carequality Implementer will make sure that its customers, network members or end users that use the Use Case services are of the type that are allowed to be Permitted Users. While we tend to think of a Permitted User as an organization or natural person, that is not necessarily a requirement. A Use Case Work Group might determine that a software system which automatically sends information qualifies as a Permitted User under a set of technical specifications. The core principle is that access is limited to Users that are known, vetted and have a legitimate reason to be using networks or services that are sponsored by Carequality Implementers.
3. ***Full Participation – Carequality Implementers will fully participate in the Use Cases that they implement.*** To encourage more robust information exchange among Carequality

Implementers and to help ensure that each Carequality Implementer (and its customers) is receiving maximum value from participation, it may be necessary to define "full" participation. Without such a definition, some Carequality Implementers may limit their use of the Use Case in a way that reduces the value of their participation to other Implementers. For example, if all Carequality Implementers implement a Use Case for one-sided use, one can quickly see that no information exchange will actually occur, therefore defeating the goals of Carequality. To avoid this undesirable situation, each Use Case Work Group will have to establish a defined level of participation in which a Carequality Implementer will have to engage in order to participate in the Use Case unless such a level of participation would be prohibited by applicable law. This level of full participation may vary based on the type of Carequality Implementer and the value that they can bring to other Implementers and receive from participation. For instance, in the Query/Retrieve Use Case, the Work Group may determine different definitions of "full" participation for those Implementers who only respond to requests (e.g. ROI vendors), for those Implementers who only submit queries (e.g. SSA), and for those Implementers who both submit and respond to queries (e.g. EHR vendors on behalf of health care provider clients). The Use Case Work Group will define "full" participation for each of these types of Implementers as well as the applicable components of the Implementation Guide.

- Example: The Query/Retrieve Use Case Work Group may determine that for Carequality Implementers that act as "responders," "full participation" means that they respond to all requests based on treatment as the permitted purpose. They may respond to requests based on other permitted purposes, but they can do so at their discretion, consistent with the Equality and Local Autonomy Principles. For purposes of this example, the Equality Principle would mean that an Implementer cannot pick and choose which other Implementers it will respond to and the Local Autonomy Principle would mean that an Implementer can refuse to respond based on its local rules, but that decision must be applied uniformly. The Work Group may further define a "response" to include both sending the requested data and sending a message that the requested data is not available. As long as the Implementer responds to messages based on treatment as the permitted purpose, it will meet its obligations to fully participate.

4. ***SLAs – Carequality Implementers will meet the service level agreements (SLAs) for each Use Case in which they participate***. Each Use Case Work Group will establish appropriate service level agreements (SLAs) for its Use Case. These SLAs may include performance expectations, system availability, response times, accuracy of matching, or data accuracy. For instance, for information in a provider directory, the Provider Directory Use Case may require that the Carequality Implementer provide an accurate list of provider names and end points/addresses. By contrast, the Query/Retrieve Use Case may require that any records exchanged be an accurate reproduction of the information in the customer's production electronic health record or other information system.

5. ***Data Sufficiency and Integrity – Carequality Implementers will transact data that is sufficient to meet the goals of the Use Case and that is an accurate representation of the data the Implementer intends to transmit.*** A key challenge with health information exchange today is the lack of consistency around what information is provided in response to a request. This challenge has two distinct dimensions:

    a. ***Data sufficiency:*** Given the absence of nationally accepted standards, there is wide variability in what information is actually provided in response to requests for information. Sometimes there is too much, non-relevant information and sometimes there is too little information. In either case, the data that is returned is of little value to the end user. A Use Case Work Group may develop specifications around data sufficiency to help ensure that data returned in response to a request is of value to the receiving end user.

    b. ***Data integrity:*** All Carequality Implementers are at different stages with respect to the electronic data that is available for exchange. In some cases, information that is sent is unreadable by the receiving software (the issue of semantic interoperability) or the information is simply gibberish. There is a general recognition that if the end-user believes that the data is not "complete" or accurate, the information will have little value and the end-users will not continue to participate in exchange and interoperability initiatives.

    In an effort to address these issues, and help ensure that the data exchanged do have value, a Use Case Work Group may adopt a minimum data set for exchange for the particular Use Case or may require that the Implementers ensure the integrity of the data that is exchanged.

    - Example 1: A Use Case Work Group may identify a minimum data set that must be transmitted in response to a request for information for purposes of treatment in connection with the administration of an immunization (assuming such transmission would not violate applicable law). The Use Case Work Group might also set a ceiling on what information is sent to avoid inundating the requestor with too much data.
    - Example 2: A Use Case Work Group may identify a different minimum data set that must be transmitted in response to a request for information for purposes of treatment in connection with a referral to a specialist (assuming such transmission would not violate applicable law). The Use Case Work Group might also set a ceiling on what information is sent to avoid inundating the requestor with too much data.
    - Example 3: A Use Case Work Group may adopt specifications related to data integrity to help ensure that data is not modified in transit.

6. ***Customizable Customer Flow Downs – Carequality Implementers must ensure that their customers agree to act in accordance with specific rules that pertain to the Use Case.*** In addition to the Universal Flow Downs described earlier**,** each Use Case Work Group may establish specific requirements that a Carequality Implementer will have to require its customers, network members or end-users to comply with. It is important that any flow downs be well thought out by the Use Case Work Group so as not to overburden Implementers with a host of changes to the Implementer's network or software.

6 DEFINITIONS

The following terms are used in these Principles of Trust and shall have the following meanings:

Applicable Law: Federal, state, territorial and tribal law that is binding on an Implementer. This includes statutes, regulations, rules, ordinances and other processes that are legally valid and enforceable based upon the legal authority of a governmental body or agency.

Customer: An organization that purchases software or services from an Implementer.

End User: The designation for a function that generates requests for information, responds to requests for information or publishes information to a list of recipients. An End User can be a natural person or it could be software that is programmed to perform these functions.

Implementer: Carequality Implementers are Networks and Service Providers that have implemented and have been verified as complying with a Carequality Implementation Guide. Companies that only license their software to customers are not Implementers.

Initiator: The party that begins a request for information. Depending on the Permitted Users rules in the applicable Implementation Guide, Implementers, End Users or Customers can all be Initiators.

Local Rule: A requirement that an Implementer has adopted to govern its network or service offering. A local rule will generally reflect a policy decision that the Implementer has made in respect of sharing information. It is not necessary that the local rule be required by Applicable Law or be based on Applicable Law.

Networks: An electronic community that operates on a single technology platform or on multiple technology platforms that are interoperable. The term "network" is construed very broadly to include health information exchange organizations (HIOs), federated nationwide networks like eHealth Exchange, and commercial health information exchange networks (e.g. Commonwell, e-prescribing networks, release of information companies, EHR vendor networks).

Responder: The party that replies to a request for information. Implementers, Customers, or End Users can all be Responders.

Service Provider: A provider of services used by networks in the conduct of health information exchange. Services may include capabilities, such as provider directories, that are hosted and

maintained by a service provider and used by networks to locate and/or identify providers, or to record locator services that are used by networks to identify locations of patient records.